ZI 2015/16

***1. Prikazan je ispis netstat s IP adresama koje su korištene u komunikaciji i portovi koji su korišteni. Pretpostavlja se da postoji bar jedan napad te je trebalo prepoznati o kojem se napadu radi i koja je IP adresa napadača.***

Odgovor je bio da je bio TCP SYN napad i da je napadač spoofao IP adresu.

***2. Navesti jedan spoofing napad na DNS***

**Early attack** ( cache poisoning ) → Korisnik želi učitati stranicu napadača, šalje upit do DNS servera, napadačev name server vrati odgovor, ali i lažnu IP adresu za neku drugu stranicu (paypal.com), Ciljani name server spremi lažnu IP adresu u cache i ljudi koji mu pristupaju dobiju krivu adresu za paypal.com

**Kaminsky DNS attack** → Napadač šalje upit za nepostojeći aaa.paypal.com i istovremeno šalje odgovore s lažnim IPom, ponavlja to dok ciljani server ne prihvati odgovor i spremi ga u cache, ljudi koji pristupaju tom serveru dobiju krivu IP adresu za paypal.com

**Napad NXDOMAIN** → Napadač preplavljuje poslužitelj upitima za nepostojeće domene, rekurzivni poslužitelj pokušava dohvatiti podatke te mu se cache popunjava rezultatima NXDOMAIN, usporava se vrijeme odziva

***// prema slajdovima spoofing != cache poisoning***

***-> cache poisoning je kompromitiranje nekog poslužitelja (njegovog cachea)***

***-> spoofing je kad se napadač predstavlja kao DNS poslužitelj,***

***ppt Infrastruktura, slajd 6***

***3. Imali smo javni i privatni ključ te smo objavili ranije javni ključ. Dobili smo mail kriptiran našim javnim ključem, ali disk na kojem je bio nas privatni ključ se uništio, možemo li dekriptirati poruku? Kako se možemo zaštiti od ovakvih događaja (što trebamo napraviti sljedeći put)? Možemo li vratiti ključeve?***

Pošto je privatni ključ trajno izgubljen, ne možemo dekriptirati e-mail bez privatnog ključa te to automatski znači da ne možemo pročitati dobivenu e-mail poruku. Možemo zatražiti novi privatni ključ, ali ne možemo nikako saznati stari privatni ključ. Sad jedino što možemo napraviti je generirati novi par koji sadrži javni i privatni ključ i napraviti backup tih ključeva.

***3. Što je RFID? Kako ugrožava sigurnost? Kako se obraniti? Što je SE?***

RFID ( Radio Frequency Identification ) jedinstveno identificira korisnika. Antena pobuđuje oznaku koja koristi EM polje antene kako bi odaslala vlastiti identifikator. Ako napadač ukrade naš RFID, može se lažno predstavljati. Zaštita: šifriranje podataka na oznaci, ograničenje dometa antene. SE (Secure Element) je sigurnosni hardware u koji se smještaju sigurnosno zahtjevne aplikacije.

***4. Što je VPN I Clientless VPN i koje je razlika između njih?***

VPN služi za sigurni udaljeni pristup intranetu te funkcionira tako da enkapsulira originalne IP pakete unutar svog vlastitog paketa, a Clientless VPN je VPN temeljen na korištenju HTTPS-a.

VPN radi na mrežnom sloju, clientless VPN na aplikacijskom ( preko HTTPS, ali može uključivati aplikacije koje koriste SSL/TLS ), clientless jer računalo već ima Web preglednik koji podržava HTTP i HTTPS.

// gdje piše da clientless radi na aplikacijskom sloju?

rekao bih da nije, clientless znači samo da ne treba imat instaliran VPN client lokalno nego se može pristupit VPN serveru putem web preglednika koji podržava HTTPS (bar prema youtube tutorialima koje sam sad gledao)

***5. Koje je implementirane sigurnosne mehanizme imao SMTP po RFC 821?***

Nikakve, podrazumijeva se povjerenje i suradnja, kasnije S/MIME.

***6. Ono sa demilitariziranom zonom i VPN sto je bilo i prošlih godina.***

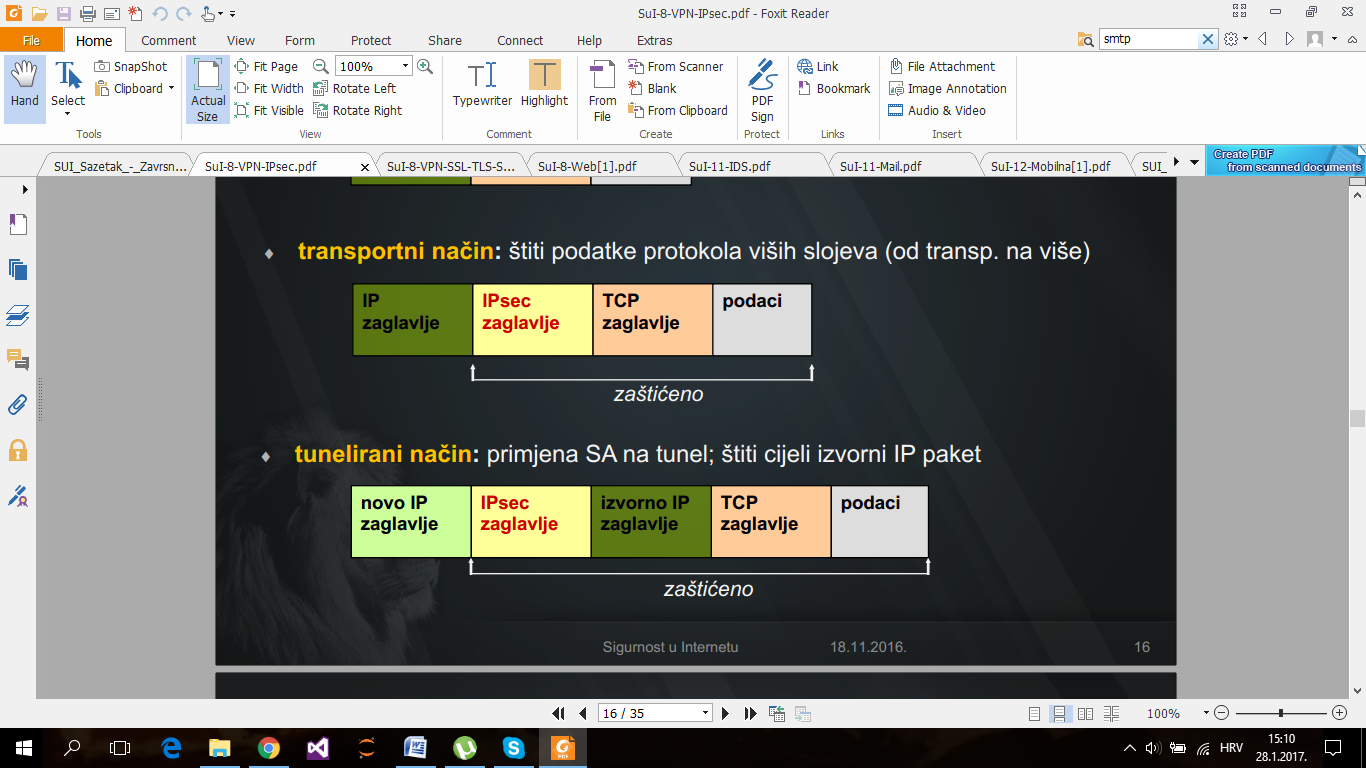
→ Radiš u firmi koja ima HTTP server i VPN. Trebaš se spojiti na mrežu tako da je veza sigurna te također mora biti prisutan i IDS (Intrusion Detection System).

***7. Kontejnerizacija(ako sam dobro napisao), opisati i navesti primjer za stolno računalo***

Kontejnerizacija je virtualna particija na uređaju na kojoj se nalaze povjerljivi podatci i aplikacije. Moguće je imati i 2 profila na uređaju, obični i sigurni. Nije moguće prebacivati podatke s jednog profila na drugi.

Primjer : Sandbox - sigurnosni mehanizam koji služi za razdvajanje okoline (u 2 profila)

***8. Razlika između transportnog ili tuneliranog IPsec?***



Transportni način štiti samo podatke protokola viših slojeva i originalno IP zaglavlje je vidljivo dok je kod tuneliranog načina cijeli izvorni IP paket zaštićen (osim novog IP zaglavlja)

***9. Zadan neki PHP kod (SQL upit), koji se napad moze izvesti i na koji način? Objasni napad!***

Može se izvesti SQL injection. To je jedna od čestih i vrlo popularnih ranjivosti koja može imati katastrofalne posljedice za aplikacije u kojima se pojavljuje. Pojavljuje se kad se nedovoljno provjereni ulazni podatci koriste za izgradnju i izvršavanje SQL upita nad pozadinskom bazom podataka. Ako korisnik unese recimo ‘ OR 1 = 1 ‘, tada će upit koji aplikacija namjerava izvršiti raditi skroz drugačiju stvar zato što je uvjet 1 = 1 uvijek istinit te će vratiti sve redove iz tablice koja se pretražuje. ***10. IPtables, pravila za dodavanje ruta, objasniti neke Itd.  
11. Kako radi antivirus, koji je to način zaštite, opisati? Kako antivirus može otkriti malware?***

Antivirus radi tako da analizira datoteke s izvršnim programskim kodom sa ciljem otkrivanja zlonamjernog koda. Oni zapravo raspoznaju samo prisutnost zlonamjernog koda u bilo kojoj datoteci na računalu.

Postoje 2 načina zaštite (i otkrivanja malwarea):

* **prepoznavanje koda /\*Prepoznavanje virusa, sl.43\*/** ( eng. *fingerprinting* ) → svaki virus ima određeni znakovni kod pa ga po tome može detektirati i nakon toga ili briše virus iz datoteke ili stavlja datoteku u karantenu ili briše inficiranu datoteku. Uspješnost ovog načina zaštite ovisi o prisutnosti znakovnog koda u bazi poznatih virusa, ali se pokazao veoma koristan zato što se najveći broj napada na sustave izvodi zapravo poznatim virusima.
* **heuristika** ( prepoznavanje ponašanja ) → nadzor ponašanja svih programa, problem je što se sumnjivim akcijama proglašavaju i one legitimne. Ova se metoda zapravo zasniva na prepoznavanju naredbi koje su označene kao potencijalno opasne, odnosno na traženju dovoljno dobrog rješenja koje ne mora davati dobar rezultat u svim slučajevima. Primjer potencijalno opasne naredbe je prepisivanje drugog izvršnog koda što može, ali ne mora biti virus.

***12. Objasnite program koji ste koristili u drugoj lab. vježbi - John the Ripper. Koje vrste napada izvršava, opišite ih? Koja je razlika između njih?***

John the Ripper je alat za probijanje lozinki koji koristi dvije vrste napada prilikom rada:

* **dictionary attack** ( napad na šifre uz poznate riječi iz svog rječnika ),
* **brute force attack** ( ako dictionary ne prođe ).

Dictionary attack napada šifru pretražujući sve riječi iz svog rječnika kojima onda pokušava probiti lozinku, dok brute force attack napada šifru isprobavajući sve kombinacije znakova (uz inkrementalno povećavanje broja znakova nakon pretrage svih kombinacija određene duljine).

***13. Koju zaštitu primjenjujemo za web aplikaciju na transportnom sloju?***

Zaštita adekvatnim mehanizmima:

* TLS na konekcijama s osjetljivim podatcima,
* šifriranje poruka prije prijenosa,
* digitalni potpis prije prijenosa.

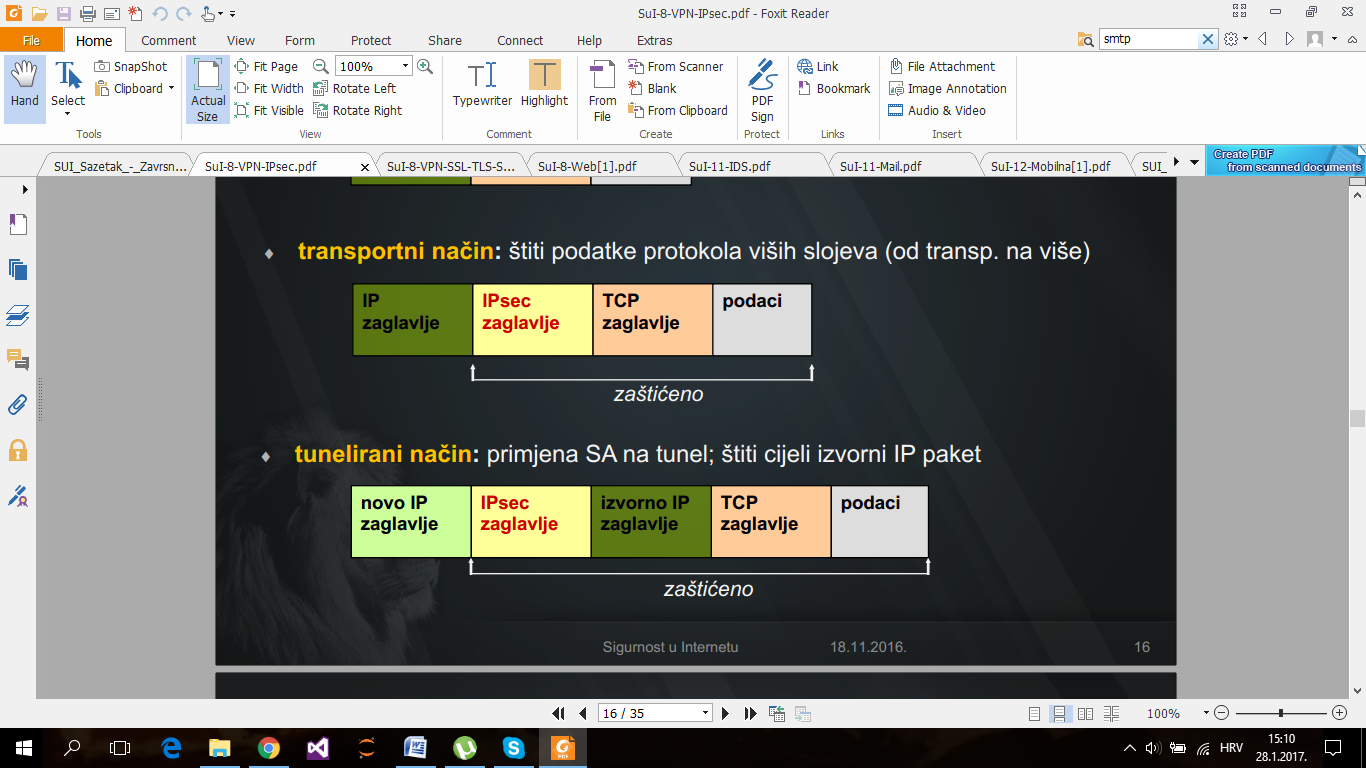
***14. Sto je NAT, kako radi i koja je njegova uloga u sigurnosti?***

NAT predstavlja prepisivanje izvorne ili ciljne IP adrese u mrežnom paketu s novom tijekom njihovog prijelaza preko usmjerivača ili vatrozida.

* u osnovi proxy jer jedan host (router) šalje zahtjeve u ime svih internih računala
* osigurava da neželjeni, neočekivani, sumnjivi podatci ne dođu do lokalnih računala
* svaki dolazni(vanjski) podatak ima izvorišnu IP adresu i port i ako se taj par IP adrese i porta ne nalazi u NAT-ovoj tablici, taj podatak neće biti propušten prema lokalnoj mreži.

ZI 2014/15

***1. netstat dana su 2 opisa, koje su razlike, koji je napad u pitanju, napadi prepoznati ih i prepoznati IP adresu napadača, mislim da je ovako a) TCP flooding jer je sve na portu 80, b) TCP skeniranje jer prolazi kroz portove 22,...,80,81,82   
2. skicirati i objasniti transportni i tunelirani način rada IPsec-a***



***3. ransomware i 3 načina kako se može dobiti***

Vrsta zloćudnog softvera koja korisniku uskraćuje pristup nekim računalnim resursima i traži naknadu/otkupninu za otključavanje resursa. 3 načina: trojanac, e-pošta, neki drugi virus…

***4. u 2.labosu smo koristili john-a. kakav je to bio napad i objasnite***

John the Ripper je alat za probijanje lozinki koji koristi dvije vrste napada prilikom rada:

* **dictionary attack** ( napad na šifre uz poznate riječi iz svog rječnika ),
* **brute force attack** ( ako dictionary ne prođe ).

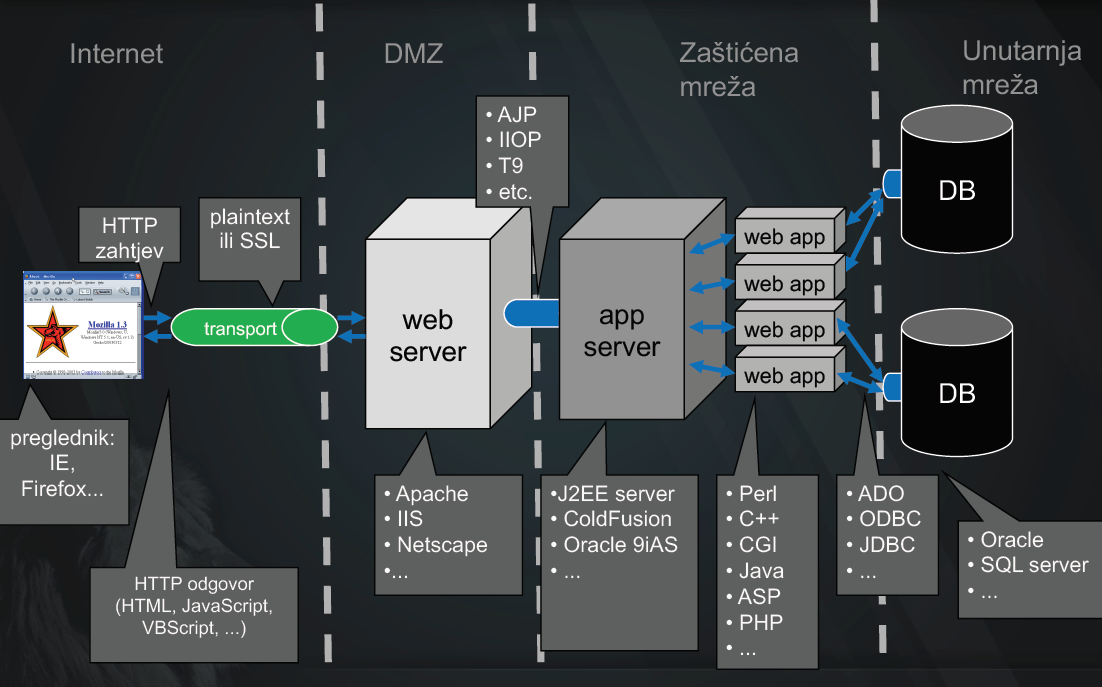
Dictionary attack napada šifru pretražujući sve riječi iz svog rječnika kojima onda pokušava probiti lozinku, dok brute force attack napada šifru isprobavajući sve kombinacije znakova (uz inkrementalno povećavanje broja znakova nakon pretrage svih kombinacija određene duljine).

***5. Opiši DNS spoofing napad. Koji je primjer takvog napada?***

napadač se pretvara da je DNS poslužitelj i šalje klijentu krive i potencijalno maliciozne informacije

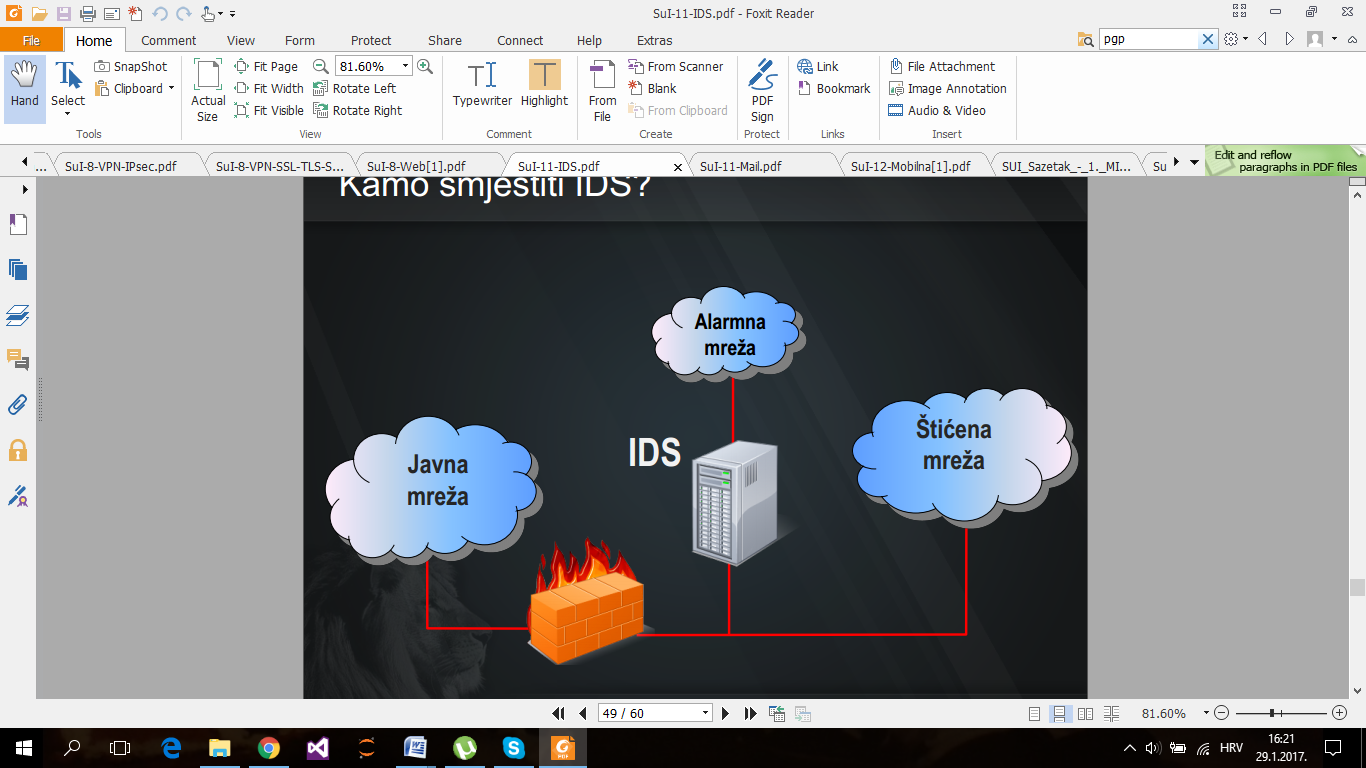
Kaminsky DNS attack

***6. nacrtano je: DMZ, zaštićena mreža, lokalna mreža a imamo: bazu podataka, web server, web aplikaciju i aplikacijski server. nacrtati to***



***7. imaš firmu, VPN, firewall, HTTP, IDS.. nacrtaj i objasni***

Ne znam točno pitanje ali IDS treba ići u alarmnu mrežu ( 49. slajd SUI-11-IDS )



***8. od prijatelja dobiš sms (koristiš android) da ideš na neki link. hoćeš li to napraviti?***

Neću. Treba provjerit sigurnost tog linka pomoću nekog antivirusnog programa. Ovakve stvari su temeljene na društvenom inženjeringu.

***9. Koje metode antivirusi koriste za zaštitu od malwarea? Objasni ih.***

2 načina zaštite: prepoznavanje koda ( fingerprinting ) -> svaki virus ima određeni znakovni kod pa ga po tome može detektirati i nakon toga ili briše virus iz datoteke ili stavlja datoteku u karantenu ili briše inficiranu datoteku

heuristika ( prepoznavanje ponašanja ) -> nadzor ponašanja svih programa, problem je što se sumnjivim akcijama proglašavaju i one legitimne

***10. kako biste osigurali neporecivost i povjerljivost prilkom slanja maila?***

Neporecivost -> digitalni potpis, povjerljivost -> asimetrična kriptografija ( kriptiranje javnim ključem osobe kojoj šaljemo mail ).

//Zašto digitalni potpis? Digitalni potpis samo rješava problem cjelovitosti jer potpis znači da smo kriptirali hash poruke. Grijesim? Da, javni ključ je dio certifikata. Ako je valjan certifikat, garantirano je da je ta osoba kriptirala svojim privatnim ključem hash poruke (ne može se poreći kriptiranje privatnim ključem).

Digitalni potpis osigurava neporecivost, mozemo zbog njega biti sigurni tko je posiljatelj

//Može li biti za oboje digitalni pečat ? pa i je, samo su u pitanju drugi potpisi, za jedno je tvoj privatni, za drugo je njegov javni

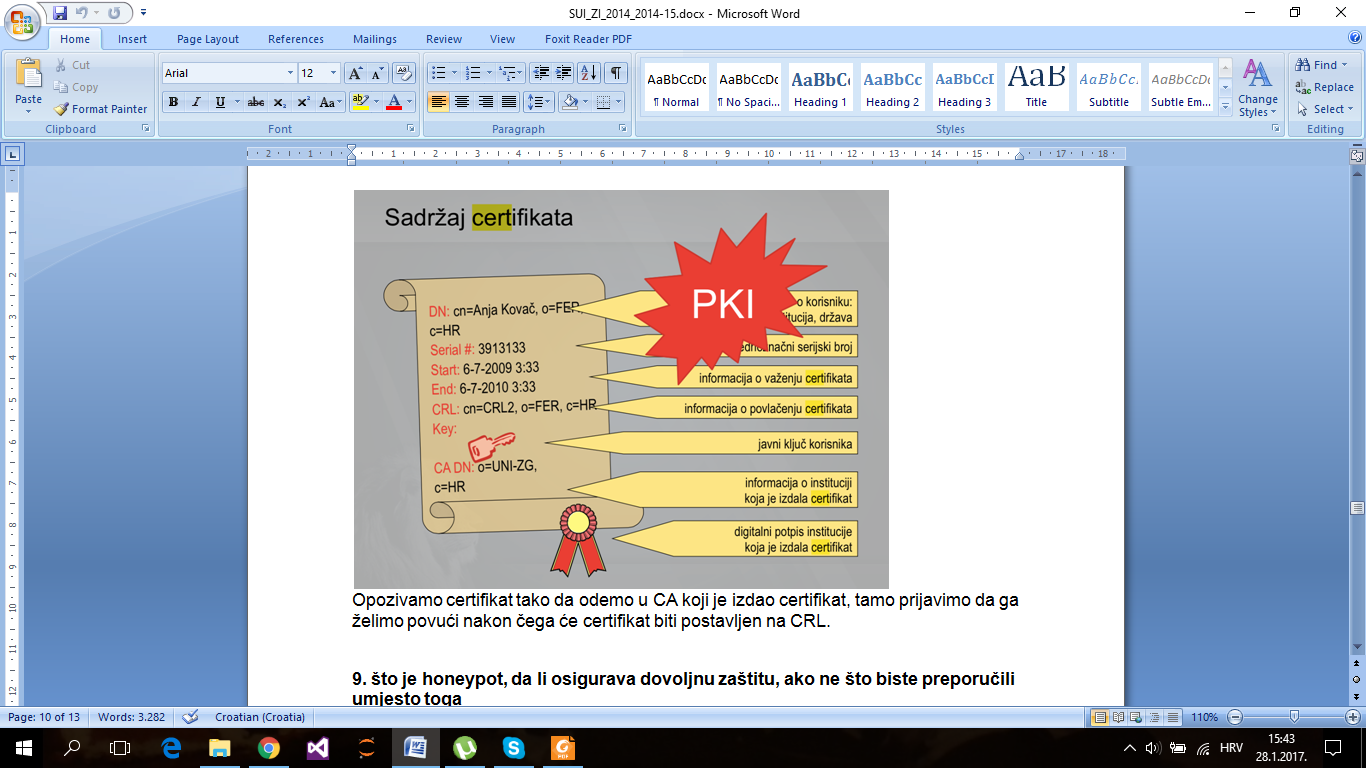
***11. što je WoT? kako se koristi u PGP-u?***

Web of Trust je model mreže povjerenja čiji je smisao mreže decentralizirana razmjena javnih ključeva. Pojedinci jedni drugima potpisuju ključeve, nema središnjeg autoriteta za potpisivanje ključeva, PGP izračunava razinu povjerenja za svaki ključ na “privjesku” ( PGP Key Ring ). Korisnici sami interpretiraju razine povjerenja.

***12. razlika signed-data i clear-signed data MIME***

Kod signed-data i sažetak i sadržaj se kodiraju prema base64 (nečitljiv tekst), a kod clear-signed-data se kodira samo sažetak

***13. koji su dijelovi certifikata? kako ćemo provjeriti važenje certifikata?***

 slika - 3. prezentacija, 8. slajd

Ili (iz nekog CARNET članka o digitalnom potpisu):

* Inačica certifikata
* Serijski broj certifikata
* Algoritam za izradu digitalnog potpisa
* Izdavač certifikata
* Valjanost certifikata (od-do)
* Vlasnik certifikata
* Korišteni algoritam za šifriranje javnog ključa
* Javni ključ
* Vrsta certifikata
* Javni ključ izdavača certifikata
* Digitalni potpis izdavača certifikata

Važenje certifikata možemo provjeriti tako da pogledamo da li je certifikat sadržan unutar CRL liste i je li istekao datum koji govori o važenju certifikata. ***14. pravila kao u 1.MI, jedno od pitanja je može li se s firewall-a pristupiti na www.google.com ako se koristi https?  
15. neki kod, prepoznati napad i opisati, SQL injection******16. Zašto je opasan RFID sniffing? Kako se od toga štiti?***

RFID ( Radio Frequency Identification ) jedinstveno identificira korisnika. Antena pobuđuje oznaku koja koristi EM polje antene kako bi odaslala vlastiti identifikator. Ako napadač ukrade naš RFID, može se lažno predstavljati. Zaštita: šifriranje podataka na oznaci, ograničenje dometa antene.

***17. Za što služi kontejnerizacija? Kako sličan princip zovemo kod računala?***Kontejnerizacija je virtualna particija na uređaju na kojoj se nalaze povjerljivi podatci i aplikacije. Moguće je imati i 2 profila na uređaju, obični i sigurni. Nije moguće prebacivati podatke s jednog profila na drugi.

Primjer : Sandbox - sigurnosni mehanizam koji služi za razdvajanje okoline (u 2 profila)

***1. Marko Č. hackira facebook, mijenja sadržaje i blokira pristup Zuckerbergu. Koja su načela sigurnosti time povrijeđena?***Cjelovitost, povjerljivost, raspoloživost.  
  
***2. Korisnik ima username i password u nekoj mreži. Kako on to može zlorabiti?***

Ako se može s time logirat na neki komp, onda može iskoristit ranjivosti operacijskog sustava i pridjelit si root prava i radit kaj hoće. (Nisam siguran za ovo, al znam da sam negdje u prezentacijama to vidio, samo mi nije jasno ovo “u nekoj mreži”. Ispravite ako griješim.) -- Malo kasno, ali dodao bih da može napraviti tunel prema nesigurnoj mreži u tu ajmo reći sigurnu mrežu (inside kriminalac).***3. Mala tvrtka postavlja IDS, a ne može ga stalno updatetati. Kakav biste im IDS preporučili i koji su rizici vezani uz njega?***  
Alat koji funkcionira na principu proučavanja nepravilnosti. Princip se temelji na tome da alat u početku “nauči” što je normalna aktivnost u mreži i da na temelju toga kasnije uočava odstupanja. Glavni rizik je potencijalno veliki broj lažnih uzbuna.  
  
***4. Što je PGP i malo ga opisati (načini razmjene ključeva, princip funkcioniranja)?***PGP je mehanizam koji osigurava povjerljivost komunikacije elektroničkom poštom s kraja na kraj. Omogućava 5 osnovnih usluga: autentifikaciju, šifriranje, sažimanje (kompresiju), kompatibilnost s infrastrukturom elektroničke pošte, segmentaciju i ponovno slaganje poruke. Povjerenje u ključeve temelji se na modelu web of trust - razina povjerenja u ključ ovisi o broju potpisa na ključu od strane korisnika s kojima je od prije uspostavljeno povjerenje.   
  
***5. U požaru je uništen jedini zapis vašeg javnog ključa (PGP). Dobili ste mailove šifrirane starim javnim ključem, hoćete li ih moći pročitati? Što treba napraviti kako bi ponovno imali sigurnu komunikaciju?***  
Moci ce se procitat mail zato jer imamo idalje privatni kljuc. Mogli bismo traziti druge da nam posalju natrag naš javni kljuc. Ubuduće bi trebali imat backup ključeva.  
\*ako je privatni uništen, nećemo moći pročitati mail i morat ćemo zatražiti nove ključeve.  
  
***6. Što je wardriving i kakve su opasnosti od njega?***  
Wardriving je pretraživanje dostupnih Wi-Fi mreža, pri čemu se napadač kreće područjem i zapisuje razine signala i GPS koordinate okolnih mreža.  
Potencijalna opasnost je otkrivanje ranjivosti dostupnih mreža.  
  
  
***7. Zašto su društvene mreže pogodnije za širenje malwarea?***  
Potencijalno maliciozni zahtjevi dolaze od mrežnih prijatelja i time djeluju uvjerljivije.  
pr. xy sent you an image.  
Morat ćeš kliknut da vidiš šta je a unutra malware!  
  
***8. Koje su (barem) dvije prijetnje najopasnije na mobitelima i koji OS je najugroženiji?***  
Bluetooth ranjivosti, malware, wardriving, RFID sniffing, uskraćivanje usluge (DoS), web aplikacije. Najugroženiji je Android, u Aziji Symbian.  
  
***9. Kako HTTP pruža potporu sjedničkoj komunikaciji, koji je OWASP napad vezan uz to i opisati i skicirati taj napad.***  
HTTP je stateless protokol. Podrsku sjednici pruza pomocu session\_id tokena kojeg klijent moze poslati kroz cookie, GET ili POST. Ukoliko se ovaj token posalje (ili ukrade) do nekog treceg klijenta, treci klijent ce imati pristup originalnoj sjednici. Najcesci propust je slanje session\_id tokena kroz GET parametar i onda (slucajno) dijeljenje svog URL-a sa sesssion-om nekom drugom. OWASP A2 - Autentifikacija i upravljanje sjednicama. Drugi slican napad, “session fixation” je kada nekome damo link koji u sebi sadrzi session token i pitamo ga da se ulogira na ranjivi servis. Kada se ulogira, mi cemo s istim linkom imati pristup njegovom racunu.  
  
***10. Dan je kod koji otvara mogućnost (u ovom slučaju) injection napada. Treba to zaključiti i opisati kako se to događa u ovom slučaju.***  
Vjerojatno se napadaču prikaže neki prozor gdje umjesto podatke, upiše SQL naredbe koje se pohranjuju u bazu i izvode kao SQL upit te dohvaćaju natrag rezultate upita koje onda napadač preuzima.   
  
***11. Koje je sigurnosne mehanizme po defaultu predviđao SMTP?***  
Nikakve. Nije postojala autentifikacija za pošiljatelja, integritet ni povjerljivost. to je riješeno sa SMTPS na transportnom sloju  
  
***12. Što je buffer overflow?***  
Preljev spremnika se dešava kada u spremnik pokušavamo pohraniti više podataka no što je kapacitet spremnika. Preljev spremnika ima razne posljedice, između ostalog i gašenje računala. Također dolazi još i do prepisivanja memorijskih lokacija koje nisu namijenjene za smještanje podataka koji se zapisuju u polje. Budući da se ostale funkcije pozivaju sa parametrima sa određenih memorijskih lokacija, ukoliko prebrišemo prave lokacije možemo upravljati parametrima drugih funkcija.  
DoS napadi u kojima se na određenu mrežnu adresu pošalje više  
prometa nego što je predvideno za tu adresu. Napadac može znati da ciljani sustav  
ima slabosti koje može zloupotrebiti, npr. da je odredeni dio sustava nezašticen ili  
napadati slucajnim odabirom. Nekoliko poznatih napada te vrste temeljili su se na  
cinjenici da sustavi imaju osnovne odredene kapacitete (default buffer). Ti napadi  
provodeni su npr. slanjem prevelikog broja ICMP paketa (poznat kao ping smrti)

***1. CIA, primjer narušavanja za svaki***    
povjerljivost(confidentiality) - čitamo nečije povjerljive podatke (npr. SMTP se prenosi u plaintextu)  
cjelovitost,integritet(integrity) - mjenjamo sadržaj nekih informacija, možemo promijeniti i sadržaj IP paketa (opet SMTP di bi mogli mjenjat sadržaj maila)  
raspoloživost(availability) - raspoloživo - DoS napad ili požar - više nije raspoloživo  
   
***3. korisnik misli da mu je narušen integritet datoteka, koji alat biste mu preporučili i da li on u potpunosti osigurava njegovo računalo***  
Preporučili bismo mu alat Tripwire koji generira sažetke svih datoteka u računalu i sprema ih u bazu podataka. Na taj način moguće je provjeriti poklapa li se sažetak sporne datoteke sa sažetkom u bazi podataka. Ako sažetci nisu jednaki datoteka je kompromitirana. Alat je moguće prevariti (npr. pomoću rootkita) stoga računalo nije u potpunosti osigurano.  
  
***4. nacrtati mrežu sa protokolima https, http, smtp koristeći sve mehanizme sigurnosti koje smo učili***  
  
***5. DNS napadi i DNSSEC***   
1. Pokvareni podaci  
2. Neautorizirana osvježenja  
3. Promijenjeni podaci o zoni, Glumljenje “mastera”  
4. Zagađenje cachea (trovanje priručne memorije)  
5. Glumljenje cachea   
  
Uvođenjem DNNSEC-a postiže se autentičnost, integritet i neporecivost DNS zapisa korištenjem asimetrične kriptografije (k

korištenjem ovakve arhitekture su znatno veći (Do 2 kbytea). Za velike odgovore moguće je koristiti TCP kao transportni protokol umjesto UDP-a.  
   
  
***6. TCP i UDP napadi***  
• TCP napadi  
"TCP overwrite"  
Varijacija napada “teardrop”. Napadač pokušava prevariti vatrozid. IP datagram se fragmentira, a TCP zaglavlje sadrži odredišni port koji vatrozid propušta. Jednom od fragmenata postavlja se pomak tako da prebriše dozvoljeni port i postavi na neki drugi port od interesa. Vatrozid treba provjeravati minimalni pomak fragmenta. - ŠTA OVO ZNAČI.  
Mislim da vatrozid provjerava taj pomak fragmenata samo za prvi paket il šta već i onda ostalo propušta, a TCP overwrite se dogodi negdje kasnije pa ga vatrozid ne vidi na vrijeme.  
  
Skeniranje TCP portova  
Ista stvar kao skeniranje UDP portova, može se lakše detektirati ali ga je najlakše izvesti. Brži od UDP skeniranja.   
  
• UDP napadi  
UDP obmana - (UDPspoofing)  
Mjenjamo izvorišnu adresu UDP datagrama i time se predstavljamo kao drugo računalo.  
  
UDP otimanje - (UDPhijacking)  
Napadač odgovara na klijentove zahtjeve UDP paketima koji imaju kao izvorišnu adresu adresu poslužitelja.  
  
UDP oluje - (UDPstorms, “UDP flooding”, “UDP DoS”)  
Najčešće se koriste servisi koji automatski odgovaraju na poruke, npr. chargen ili daytime. Lažira se UDP paket na način da mu se pod izvorišnu adresu stavi adresa žrtve, a pod izvorišni port port jednog automatskog servisa. Takav datagram se šalje na neko drugo računalo također na port automatskog servisa. Računala si tako automatski odgovaraju u bekonačnost.  
  
Skeniranje UDP portova   
Napadač pokušava otkriti koji se sve servisi vrte na računalu. Ako je port zatvoren, sustav može ali i ne mora odgovoriti porukom ICMP port unreachable. Ako odgovori onda je port sigurno zatvoren, ali ako ne odgovori ne možemo biti sigurni da nije zatvoren. Tehnika je spora.  
  
***7. neki kod zadan, i trebalo je napisati na koje napade je izložen i kako ih spriječiti***

***8. digitalni certifikat što sadrži, kako ga opozvati, što sadrži javni ključ***Opozivamo certifikat tako da odemo u CA koji je izdao certifikat, tamo prijavimo da ga želimo povući nakon čega će certifikat biti postavljen na CRL.  
  
***9. što je honeypot, da li osigurava dovoljnu zaštitu, ako ne što biste preporučili umjesto toga***-oponašanje dobro poznate rupe u zaštiti, predstavlja žrtvu napada  
-ne osigurava dovoljnu zaštitu  
-  
-nedostaci:  
o prate napad usmjeren samo na njih  
o napadači ih mogu preuzeti  
- prevencija:  
o usporavaju ili zaustavljaju napad  
o zbunjuju napadača  
- otkrivanje:  
o sav promet usmjeren njima po definiciji je sumnjiv  
- reakcija:  
o lako se ustanovi što je bio cilj napada jer se bez posljedica sustav može analizirati  
  
***10. što je hash, za šta služi i primjer korištenja***    
Hash je funkcija kojom se podaci hashiraju :) tj bitno promijene te je gotovo nemoguće ponovno otkriti početne podatke (one-way hash).  
Služi npr. kod pohrane passworda gdje se izgenerira hash od unesenog passworda, spremi, te pri svakom idućem pokušaju autorizacije hash se ponovno generira i uspoređuje s onim prvim hashom.  
Primjena: digitalni potpisi, autentifikacija, hash-tablice, checksum  
Hash je funkcija kojom se stvara sažetak poruke. Ulaz je proizvoljno dug tekst, a izlaz je fiksne duljine. Koristi se kod digitalnog potpisa, autentifikacije, za provjeru kontrolne sume. Hash je jednosmjerna funkcija što znači da iz izračunatog hash-a nije moguće dobiti izvornu poruku.

***2. Primite poruku koja je šifrirana simetričnim ključem te uz nju dobijete taj isti simetrični ključ šifriran asimetričnim ključem (vašim javnim). Što morate napraviti kako biste pročitali dobivenu poruku?***  
Potrebno je prvo našim privatnim ključem dešifrirati taj simetrični ključ i onda tim dešifriranim simetričnim ključem dešifrirati poruku. To je hibridni pristup.  
  
***3. Dana dva ispita s netstat i iz njih treba prepoznati dva TCP napada te otkriti napadačevu IP adresu.***  
  
***4. Uočite nagli porast konekcija s protokolom UDP i ARP u petak i onda još preko vikenda to podivlja. O kojem se zloćudnom programu radi? Koji su glavni dijelovi tog zloćudnog programa? Kojim protokolom od navedenih se on vjerojatno širio?***  
Riječ je o crvu koji se širi UDP-om.

Glavni dijelovi: bojna glava, pogon, mehanizam odabira mete, sustav za odabir mete, korisni teret.  
  
***5. Napišite na kojim slojevima TCP/IP složaja se nalaze uređaji te označite koji su podložni prisluškivanju:***  
router - mrežni, podložan  
switch - podatkovni, podložan  
hub - fizički, podložan  
  
***6. IPFW naredbe, prepoznati što koja radi. Jedna je bila i s STATE ESTABLISHED, tako nešto. Prepoznati podmreže s kojih se može pingati poslužitelj. Mogu li se slati HTTP zahtjevi na poslužitelj?***  
Nešto ovako: -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT   
Hvala kolegi j0p@.  
  
1) Propustaju se ulazni paketi koji nisu novi nego pripadaju vec postojecoj konekciji  
2) Propustaju se ulazni paketi koji dolaze od zadane podmreze prema portu 22  
3) Posluzitelj se moze pingati sa podmreza koje su navedene u pravilu oblika INPUT -p ICMP ACCEPT  
4) Ne mogu se slati zahtjevi na posluzitelj jer ne postoji pravilo koje prihvaca pakete prema portu 80  
  
***8. U vašoj firmi se gura BYOD (Bring your own device) jer svi zaposlenici imaju smartphoneove. Navedite 3 moguća sigurnosna problema koji bi mogli utjecati na mrežnu strukturu. Kako bi se taj problem mogao riješiti?***  
-pristupa se podacima tvrtke koji ostaju na mobitelu i nakon što zaposlenik otiđe iz tvrtke i može ih netko ukrasti  
-lako izvođenje phising napada na BYOD uređajima  
-veća ranjivost na malware koji mogu krasti informacije kad se zaposlenik spoji na wi-fi  
-laka provala u uređaj pri njegovu gubitku  
Može se riješiti instalacijom antivirsunog programa ili kontejnerizacijom, gdje će uređaj imati dva profila – sigurni i obični te podatke nije moguće prebacivati iz jednog u drugi.  
  
***9. Korisnik pri prijavi na aplikaciju dobiva Session ID. Može li se autentifikacija osloniti u potpunosti samo na HTTP protokol? Ako da, zašto, ako ne, zašto ne?***Gdje se sve može spremiti Session ID?  
-ne, autentifikacija se izvodi preko SSL-a čime se dobiva sigurniji HTTPS  
-SESSION ID se vidi na mreži, u pregledniku, u logovima, a može se spremiti i u URL čime se izvodi loša autentifikacija  
-rj: novi SESSION ID kod svakog zahtjeva  
  
***10. Dana dva različita sažetka. Jedan je dobiven izračunom nad skinutom instalacijskom datotekom, a drugi je došao uz datoteku. Hoćete li pokrenuti tu instalacijsku datoteku. Ako da, zašto da, ako ne, zašto ne? Možete li iz sažetka rekonstruirati instalacijsku datoteku? Ako da, zašto da, ako ne, zašto ne?***  
-ako sažeci (hash) nisu jednaki, znači da je ubačen virus, pa nećemo pokrenuti datoteku  
-iz sažetka se ne može rekonstruirati instalacijska datoteke, jer je hash jednosmerna funkcija (pogledaj hash :D)  
  
***11. Dan je neki pseudo/php kod sličan ovom koji obrađuje formu, $komentar je unos korisnika:  
html kod:  
public function dodajZapis($komentar)  
{  
 $komentar = počisti($komentar);  
 $rezultat = mysql\_upit('INSERT INTO komentari (komentar) VALUES (\'$komentar\')');  
}  
public string počisti($komentar)  
{  
 $komentar = ukloni\_sve("<script>", $komentar);  
 $komentar = ukloni\_sve("</script>", $komentar);  
 return $komentar;  
}***  
Kakav napad se može napraviti? Može li se kakav drugi način injectiona koristiti i kako?  
  
Ovaj kod je podložan SQL Injectionu tako da možemo dumpat cijelu bazu ako si damo truda. Također, miču se jedino script tagovi tako da možemo ubacivat html kod što isto nije ok.

Mogao bi CSS attack (uvijek možeš na neki element koji nije script stavit neki onclick, onhover i ubacit nekakvu funkciju koja će se izvršit)  
  
***12. Što je Same origin policy? Zašto se unatoč njoj može provesti CSRF?***  
Od prvih inačica funkcija XHR izvedena je tako da poštuje tzv. „same origin“ pravilo. Riječ je o pravilu koje zahtjeva da se web zahtjevi mogu pokretati samo nad stranicama iz kojih su učitani. Tako je web odredište s kojeg se učita programski kod jedino odredište prema kojem mogu biti upućeni zahtjevi za sadržajem koji je dio učitanog koda. Na taj način otklanja se mogućnost CSRF napada. Ipak, valja napomenuti kako samo pravilo istog izvora i odredišta ne jamči potpunu sigurnost. Može se zaobići manipulacijama DNS-om ili skrivanjem pravog izvora zahtjeva posebnim oblikovanjem HTML-a. Primjer takvog oblikovanja može biti manipulacija „Referer“ zaglavljem koje sadrži informaciju o izvoru poruke. Razvojem Web 2.0 tehnologija sve je naglašenija potreba za komunikacijom između web odredišta bez interakcije korisnika, odnosno za odbacivanjem „same origin“ pravila. Time se otvaraju naprednije mogućnosti oblikovanja web sustava i usluga, ali se i povećava opasnost od CSRF i drugih napada.   
(kopirano s carnetove stranice)

USMENI

stuxnet(navodno neki crv iz predavanja, kao napad na iranska nuklearna postrojenja), ransomware kako funkcionira, smtp, Security element i prosirenje smtp i nat.

Stuxnet, CSRF, Injection (SQL injection, Script (code) injection), Sigurnosni elemnt, Virusi, Ransomware (i koji ključevi), SMTP, eSMTP, NAT, XSS…

OS fingerprinting, Injection(uz to malo po 4.labosu), randsomware

Bio kod Mikuca u 11. Prvo me pitao radim li sto izvan FERa vezano za servere i Web, kad sam rekao da pitao me kako sam zastitio to od onih tipicnih napada sa 3. labosa. Onda me pitao DDoS sto je i kako se sve moze izvesti. Kada pošaljem mail koje sam one karakteristike ispunio (cjelovitost bla bla bla, trik pitanje nikakve) i jos me pitao kako ono s treceg labosa funkcionira slowloris za DoS.

Kada se otvori fer.hr objasniti zašto je https i zašto je zelen i što to znači te kako to preglednik prepozna.  
DNS i DNSSEC. Treba reći i da se podaci digitalno potpisuju privatnim ključem kod DNSSEC.  
DoS i DDoS, smurf, reflected (amplified) i primjer.  
Što je IP spoffing i što se može s njime?

- stuxnet. O čemu se radi i kako je uspio ući (pitanje je zapravo na koji način je moguće sve)? Malo se prebacio onda i na načine zaraze mobitela. Kako antivirusi rade?  
- SSL/TLS te PKI i certifikati. Kako ide komunikacija između 2 računala? Diffie-Hellman algoritam za razmjenu ključeva. Što je to PKI? Šta sadrži certifikat?  
- objasniti mrežni napad po želji   
- CSRF  
- Hashiranje (salt)

Ping, nmap, certifikati

kako bi poslala mail da ga nitko ne može pročitati? ->objasniti asimetričnu kriptografiju; šifriranje tokova, One-time-pad; izgubljen je privatni ključ-što treba napraviti, može li se doći do poruke?; objasniti SYN flood; Web of trust.

IP spoofing (objasniti kako radi, koji je cilj, kako se možemo zaštititi), ping, TCP skeniranje, TCP napadi

udp amp na primjeru, tcp skeniranje portova i kod certifikata, kako se provjerava crl

dmz, dnssec, arp napad

STARI MEĐUISPITI (treba provjeriti)

(za pitanja iz 1. ciklusa koja bi se mogla ponoviti)

→ ovo sam samo kopirao šta sam imao ispunjeno dok sam se spremao za MI, moguće (vjerojatno) je da ima grešaka, ja sam planirao stare ispite prolaziti malo kasnije pa ću tad vjerojatno i ispraviti/nadopuniti

# MI 2011/12

**1. Objasni što je neporecivost i kako bi se osigurala neporecivost preko e-maila?**

Neporecivost je sigurnosni zahtjev kojim se osigurava da sudionici ne mogu odbiti ili poreći akciju u kojoj su sudjelovali.

Neporecivost bi se preko e-maila osigurala koristeći digitalni potpis čija bi prisutnost bila dokaz da je osoba koja je poslala neku e-mail poruku sudjelovala u toj radnji.

**2. Usporedi tokove i blokove podataka te navedi po 1 primjer algoritma za svaki.**

Tokovi i blokovi podataka se koriste kod simetričnih algoritama. Tokovi podataka se šifriraju bit po bit, dok se kod blokova podataka operira nad blokovima stalne dužine.

Primjeri algoritama:

· Tokovi:

o GSM – A5, one time pad

o TLS ili WEP – RC4

o RC4, A5/1, A5/2, Helix, WAKE

· Blokovi podataka:

o DES, 3DES, AES, Blowfish/Twofish...

**3. Što se sve mora provjeriti kako bi se utvrdila valjanost certifikata?**

Informacije o korisniku: ime, institucija, država; jednoznačni serijski broj, informacija o važenju certifikata, informacija o povlačenju certifikata, javni ključ korisnika, informacija o instituciji koja je izdala certifikat, digitalni potpis institucije koja je izdala certifikat.

**4. Kako se naziva software s namjenom preuzimanja korisničkih podataka i navedi 2 metode koje koristi?**

Naziva se Spyware. Osobni podaci se tajno prikupljaju koristeći razne metode: nadzorom pritisnutih tipki na tastaturi, pohranjivanjem adresa Web-sjedišta koje korisnik posjećuje ili analizom dokumenata na tvrdom disku korisnika.

**5. Može li se za digitalni potpis koristiti simetrično šifriranje i obrazloži?**

Ne može se koristiti simetrično šifriranje zato što samo pošiljatelj ima ključ kojim je poruka potpisana, dok bi se korištenje jedinstvenog ključa bilo tko mogao potpisati.

**6. Čemu služi hash i navedi 2 primjera algoritma?**

Hash služi za generiranje sažetka poruke prije digitalnog potpisivanja. Primjeri algoritama su: Message Digest Algorithm 5 (MD5), Secure Hash Algorithm (SHA-1), Secure Hash Algorithm (SHA-2, SHA-3).

**7. Ukratko objasni DNSSEC**

DNSSEC (Domain Name System Security Extensions) je tip zaštite infrastrukture koji osigurava kriptografski dokaz ispravnosti primljenih podataka. Temelji se na korištenju asimetrične kriptografije, javnih i privatnih ključeva te se njime osigurava valjanost podataka između autoritativnog poslužitelja i resolvera. Podatcima se može vjerovati samo u slučaju kad je root (.) potpisan!

**8. Navedi 2 napada koji koriste TCP SYN zastavicu. Kojom se naredbom mogu otkriti? Što se izvršavanjem te naredbe ispisuje?**

Skeniranje portova i SYN preplavljivanje. Skeniranje portova šalje paket SYN te se još naziva i poluotvoreno skeniranje. Koristi se za prikupljanje informacija o žrtvi radi pronalaženja slabosti i time mogućnosti za napad. Ako dobijemo paket RST, port nije otvoren, a ako dobijemo paket SYN/ACK, tada je port otvoren.

Kod SYN preplavljivanja se šalju SYN segmenti s izmijenjenom IP adresom pošiljatelja. Pošto izmijenjena IP adresa odgovara nepostojećem računalu, žrtva nikada neće primiti odgovor na svoj SYN/ACK paket te će doći do DoS-a: ostaju poluotvorene konekcije.

Mogu se otkriti koristeći naredbu **netstat** te se izvršavanjem te naredbe ispisuje mrežna statistika tijekom nekog prometa u mreži, tablice usmjeravanja i broj mrežnih sučelja. Pošto bismo primijetili veliki broj poluotvorenih konekcija sa SYN\_RCVD stanjem, tako bismo otkrili da je došlo do napada.

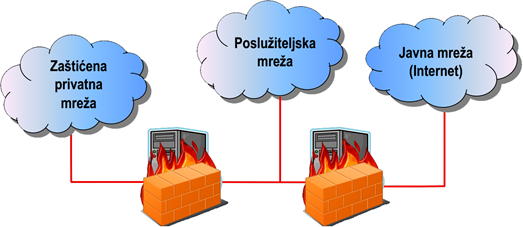
**9. Usporedi kako se šire virusi, crvi i trojanci?**

Virusi i trojanci se ne šire samostalno te se šire isključivo djelovanjem korisnika, dok se crvi šire samostalno.

**10. Radite u tvrtki koja ima poslužitelj za http i smtp zahtjeve. Treba omogućiti zaštitu privatne mreže uz dostupnost poslužitelja javnoj mreži. Kako biste posložili mrežu? Skicirajte.**

Privatne mreže s uslugama za vanjske korisnike - “Demilitarizirana zona”

Privatna mreža – FIREWALL – Poslužiteljska mreža – FIREWALL – Javna mreža



**11. Screenshot firewall buildera i objasniti: recimo prvi i zadnji red - što je prikazano? Koje sve portove i protokole će klijent imati otvorene prema van i još nešto**

Prikazan je skup pravila koja govore što sve vatrozid propušta. Prvi red prikazuje pravilo što se radi s eth0 vanjskim sučeljem (u ovom slučaju se zapisuju svi paketi koji dolaze izvana), dok zadnji red prikazuje skup pravila koji zapisuju sve pakete koji nisu odbačeni te za svaki slučaj sve ostalo što ostane odbacuje. Imat će otvorene HTTP, SSH, DNS, SMTP protokole, dok će biti otvoreni portovi 22, 25, 53 i 80.

**12. Usporediti napade na hub i switch. Navesti primjere napada na njih i na kojem se OSI sloju nalaze**

Kod napada na hub napadač može vidjeti sav promet koji se događa na segmentu koji pregledava jer ga hub šalje svim računalima u mreži, dok se kod napada na switch promet ne šalje svim računalima u mreži (komutator održava tablicu s MAC adresama / portovima te šalje promet na točno određeno računalo prema tablici). Primjer napada na hub je njuškanje mreže/prisluškivanje, dok je primjer napada na switch MAC flooding ili MAC duplicating/cloning. Hub se nalazi na fizičkom sloju, dok se switch nalazi na podatkovnom sloju.

# MI 2012/13

**1. Što je cjelovitost i kako bi ju ostvarili u mreži?**

Cjelovitost je osnovni sigurnosni zahtjev koji postavlja kao cilj informacijskog sustava da se zaštite podatci od neovlaštenog brisanja, mijenjanja ili bilo kakve manipulacije bez prethodne autorizacije u mreži. Ostvarila bi se dodjelom samo nužnih prava pristupa, odvajanjem dužnosti tako da se raspodijeli odgovornost nad ključnim dijelovima procesa na bar 2 fizičke osobe i rotacijom dužnosti.

**2. Dobio si usb za koji znaš da ima neki malware ali ne znaš je li virus, crv ili trojan. Što smiješ a što ne smiješ napraviti?**

Ako je crv, ne smijemo uštekati USB jer će se računalo odmah zaraziti te će se crv razmnožavati i dalje širiti. Ako je virus ili trojanac, smijemo uštekati USB jer moramo pokrenuti program ili datoteku gdje se nalazi virus ili trojanac da se računalo zarazi. Virus se onda širi sam, dok se trojanac ne širi.

**3. Koja je razlika između skeniranja portova sa TCP SYN i napada TCP SYN flood?**

Skeniranje portova šalje paket SYN te se još naziva i poluotvoreno skeniranje. Koristi se za prikupljanje informacija o žrtvi radi pronalaženja slabosti i time mogućnosti za napad. Ako dobijemo paket RST, port nije otvoren, a ako dobijemo paket SYN/ACK, tada je port otvoren.

Kod SYN preplavljivanja se šalju SYN segmenti s izmijenjenom IP adresom pošiljatelja. Pošto izmijenjena IP adresa odgovara nepostojećem računalu, žrtva nikada neće primiti odgovor na svoj SYN/ACK paket te će doći do DoS-a: ostaju poluotvorene konekcije.

**4. Koja je razlika između koncentratora i komutatora u smislu prisluškivanja prometa? Što se može izvesti da bi se prisluškivanje odvijalo jednako i na komutatoru i na koncentratoru?**

Kod napada na hub (koncetrator) napadač može vidjeti sav promet koji se događa na segmentu koji pregledava jer ga hub šalje svim računalima u mreži, dok se kod napada na switch (komutator) promet ne šalje svim računalima na mreži (komutator održava tablicu s MAC adresama / portovima te šalje promet na točno određeno računalo prema tablici). Možemo nad komutatorom izvesti MAC flooding gdje se komutator preoptereti s krivim MAC adresama tako da mu se prepuni tablica te tada komutator najčešće prelazi u hub način rada.

**5. Kod**

**int main (int argc, \*\*char argv)**

**{**

**s=char[256]**

**....**

**strcat(s, argv[1]);**

**system(s);**

**...**

**}**

**Koji napadi bi se mogli izvesti s obzirom na kod? Kako bi spriječio te napade?**

Može se izvesti buffer overflow koji možemo spriječiti tako da prije dodjeljivanja znaka polju s provjeravam duljinu ulaznog niza tako da ona slučajno ne premaši duljinu koja je jednaka 256.

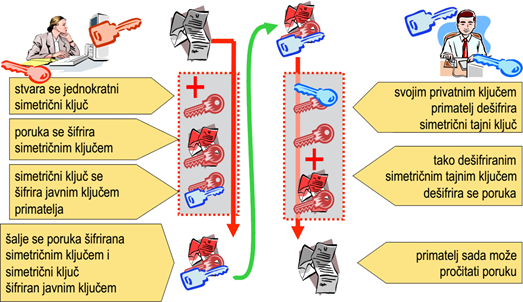
**6. Ispis pravila za vatrozid (ono tipa from any to any i te šeme) i pitanja o nekim pravilima šta znače?**

**WebPoslužitelj ima otvorenu mogućnost slanja TCP paketa prema vanjskoj mreži. Kako vatrozid zna da je TCP paket koji dođe izvana onaj odgovor kojeg WebPoslužitelj čeka?**

Kreiranjem dinamičkih pravila za TCP konekciju iniciranu “iznutra” omogućuje se propuštanje odgovora iz vanjske mreže.

Zato što firewall čeka odgovor na tom portu (ako je uključen keep-state).

**7. Kako bi korištenjem simetričnog i asimetričnog algoritma kriptirao poruku?**



**8. Koja je razlika u šifriranju tokova i blokova? Ako se promijeni jedan bit u šifriranom što se dogodi kod tokova a što kod blokova?**

Tokovi podataka se šifriraju bit po bit, dok se kod blokova podataka operira nad blokovima stalne dužine. Ako se promijeni jedan bit u šifriranom tekstu, kod tokova dolazi do greške zato što mora postojati sinkronizacija na obje strane, dok kod blokova ne dolazi do greške zato što se blok bitova preslikava iz otvorenog koda u blok bita šifrata jednake veličine koristeći ponavljajuću funkciju i ključ.

**9. Opiši Kaminsky napad? Može li se on spriječiti DNSSEC-om? Objasni.**

Napadač šalje DNS upit za neku nepostojeću adresu, npr. aaa.paypal.com. Također odmah šalje lažne odgovore na vlastiti upit te svaki odgovor sadrži drugi ID upita i lažnu IP adresu za [www.paypal.com](http://www.paypal.com/). Napadač ponavlja korake 1 i 2 s različitim prefiksima: aab.paypal.com, aac.paypal.com, … sve dok ciljani server napokon ne prihvati lažni (spoofani) odgovor. Taj lažni odgovor tada „otruje“ cache imenovanog servera s lažnom adresom za [www.paypal.com](http://www.paypal.com/). Zbog toga su korisnici koji pristupaju [www.paypal.com](http://www.paypal.com/) preko zaraženog imena servera preusmjereni na web-stranicu koja izgleda kao PayPal, ali ona radi samo tako da sprema njihova korisnička imena i lozinke. DNSSEC može biti rješenje za Kaminsky napad pošto on osigurava kriptografski dokaz ispravnosti primljenih podataka, ali se i u tom slučaju prikazanoj stranici može vjerovati samo u slučaju da je root (.) potpisan!

**10. U kompjuteru se lozinke korisnika pohranjuju u bazu kao sažetak lozinke (hash). Kako bi spriječio napad rječnikom u offline modu?**

Napad rječnikom u offline modu možemo spriječiti koristeći SALT. Lozinke se hashiraju tako da se uz lozinku u /etc/shadow dodaje i slučajno generirani hash. Korisnici s istom lozinkom imaju različiti hash.

**11. Osnivamo tvrtku i imamo http, https i ssh poslužitelje. Želimo da ti poslužitelji budu raspoloživi vanjskoj mreži, ali da unutarnja mreža u isto vrijeme bude zaštićena. Skicirajte kako bi to ostvarili i objasnite.**

Isto

# MI 2013/14 - samo nova pitanja

1. Zadan je sažetak iz SHA skupine sažetaka bio je duljine 56 znakova

· gdje bi se mogao takav sažetak koristiti? kod digitanog potpisivanja, kontrolna suma

· koje sigurnosne zahtjeve možemo s njim ostvariti? cjelovitost

· kojem se sažetku točno radi → 56 znakova? 224 bita → SHA2

2. Zadatak je išao ovak nekak: prijatelj vam je preko maila u datoteci poslao ovo: ….. i sad su napisali javni ključ

· što je sadržano u datoteci? kriptirana datoteka

· kako ćemo dalje postupiti? dekriptirat ću javni ključ svojim privatnim ključem koji ću dekriptiran iskoristiti za dekriptiranje datoteke

· hoćemo li vjerovati potpisu? provjeravamo sažetak (checksum) i ako odgovara stvarnom, vjerujemo … inače ne

· možemo li s njim digitalno potpisati dokument? ne možemo

**3. objasniti namjenu protokola ARP? na kojem TCP/IP sloju se nalazi? može li se i kako zloupotrijebiti da se ugrozi mreža?**

ARP (Address Resolution Protocol) je protokol za pretvaranje 32-bitnih IP adresa u 48-bitne Ethernet (MAC) adrese te se nalazi na sloju podatkovne poveznice. Može se zloupotrijebiti na sljedeće načine: slanjem odgovora prije pravog računala te vraća lažno preslikavanje adresa, slanje lažnih ARP upita koji se koriste za spremanje krivih ARP preslikavanja na računalu kome se upućeni, slanje ARP poruka kontinuirano tako da bi se lažni podatci zadržali u cacheu, preusmjeravanje prometa koji bi trebao ići na usmjeritelj te ga se može u potpunosti filtrirati, lažno preslikavanje gatewaya u nepostojeću MAC adresu – DoS napad.

**4. moramo osigurati prijenos zvuka u stvarnom vremenu. koju metodu ćemo koristiti- tok podataka ili blokove i zašto? navesti primjer algoritma koji bi koristili?**

Koristit ćemo tok podataka zato što bitovi konstantno dolaze pa time osiguravamo da ih možemo odmah rekonstruirati. Primjeri: RC4, A5/1, A5/2, Helix, WAKE.

**10. napisati karakteristike 509.X potpisa**

# MI 2014/15 - samo nova pitanja

**1. Razlika u skeniranju portova UDP i TCP protokola?**

Kad skeniramo UDP portove, dobivamo poruke (ICMP) uglavnom kad je port zatvoren, dok kod TCP protokola ovisno o metodi skeniranja dobivamo neki paket kao odgovor (ovisno o metodi skeniranja i ako je port otvoren ili zatvoren).

# MI 2015/16 - samo nova pitanja

**1. Objasniti digitalni potpis, sto je očuvano digitalnim potpisom i protokoli koji su korišteni za dig. Potpis u labosu?**

Prema načelu digitalnog potpisa, pošiljatelj potpisuje poruku koristeći svoj privatni ključ. Potpis mogu verificirati svi koji imaju javni ključ pošiljatelja. Digitalnim potpisom su očuvani neporecivost, autentičnost i cjelovitost. Protokol ???

**2. Razlika između ECB i CTR, navesti primjere asimetričnih algoritama.**

Kod ECB-a se blokovi šifriraju nezavisno te nije potreban inicijalizacijski vektor, dok se kod CTR-a blokovi šifriraju nezavisno te je u upotrebi inicijalizacijski vektor.

**3. Izračunati vrijeme napada rjecnikom prije korištenja brute-force metode ako imamo svoj rječnik od 15000000 rijeci i napadamo datoteku od 60000 rijeci gdje su spremljeni hash zapisi, svaki sa različitim SALTom, trajanje hash funkcije je 1ns**

**4. Kako se provjerava valjanost certifikata?**

**5. Gdje su u sustavu(unix) spremljeni Podatci o korisniku i lozinke? Primjer zapisa, trebalo objasnit**

Nalaze se u /etc/passwd. ?

Man In The Middle – svi čvorovi mogu biti krivo konfigurirani: DoS ili presretanje prometa