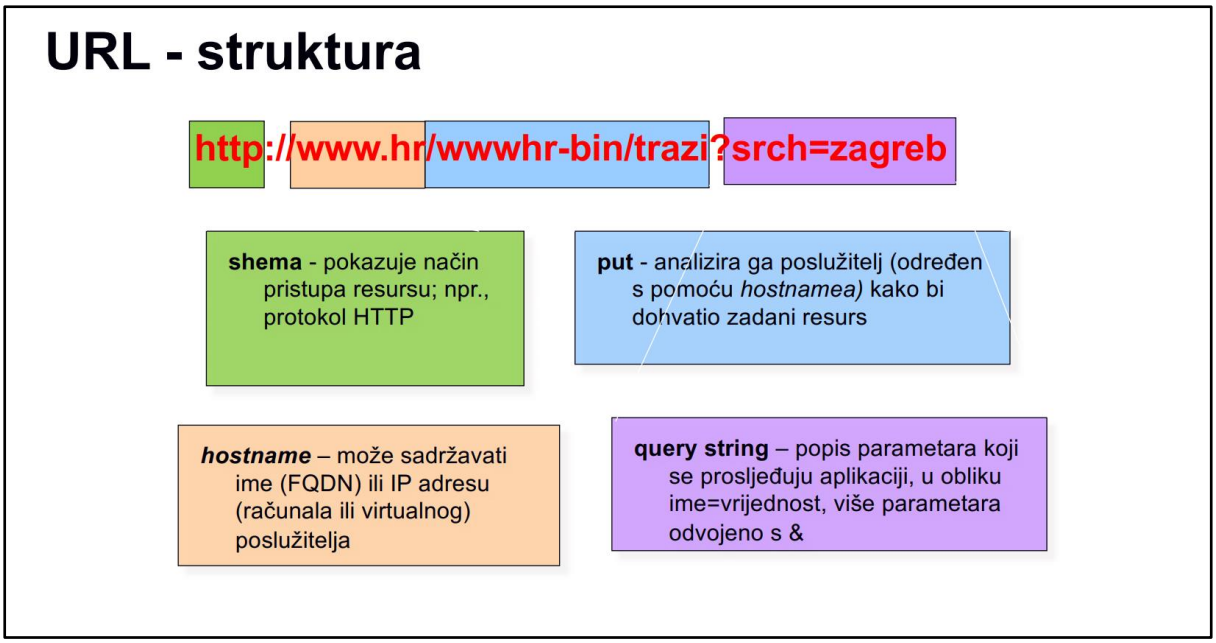
SRS Završni ispit

Sigurnost web aplikacija

- **Dvije strane sigurnosti web aplikacija**
  1. Preglednik (na klijentu)
     - Napadi koji iskorištavaju ranjivosti preglednika
     - Posljedice
       - Instalacija malwarea
       - Krađa dokumenata u korporativnim mrežama
       - Gubitak privatnih podataka
  2. Aplikacija (na poslužitelju)
     - Potencijalne rupe: XSS, XSRF, SQL injection
     - Posljedice
       - Ukradeni brojevi kreditnih kartica
       - Krađa podataka
- **Lokot u pregledniku**
  - Autentifikacija poslužitelja – sve treba biti zaključano
  - Kada koristimo HTTPS, svaki poslužitelj weba treba imati važeći certifikat
  - Preglednik provjerava taj certifikat i zaključava lokot ako je sve u redu
- **IDN Homographic Attack**
  - IDN - internationalized domain name
  - URL može sadržavati unicode znakove
  - Važno -> certifikat/lokot su zeleni
  - Korisno za phishing napade
- **HTTP protokol**
  - Stateless – ne održava stanje
  - Problem -> web-aplikacija mora održavati takve podatke
  - Rješenja
    - postavljanje i slanje cookieja
    - korisničke sjednice (sessions)
    - skrivene varijable (unutar obrazaca)
    - parametri kao dio URL-a
  - komunikacija nije šifrirana!
- **HTTP autentifikacija**
  - Razine
    - Basic (plaintext - nesigurno)
    - Digest (hash lozinke - replay napad)
    - NTLM (sigurnije, ali upitna podržanost u preglednicima)
  - Preglednik klijenta pamti ime i lozinku (ne cookie!)



Slika 1 URL struktura

Ranjivost web aplikacija

1. **Umetanje (injection)**
   - Uključuje tekst (zapravo naredbe, SQL upite i slično) i prosljeđuje ih aplikaciji
   - Aplikacija uzima takve ulazne podatke i interpretira ih kao naredbe ili upite
   - Jednostavno za izbjeći
   - Opasan – moguća je kompromitacija ili promjena cijele baze podataka
   - Vrste
     - Tautologija
       - Iskaz koji je u svakom slučaju istinit
       - Primjer naredbe SELECT first_name, last_name FROM users WHERE user_id = 'any' OR '1'='1'
     - Ilegalni upiti
       - Različitim SQL naredbama pokušavamo vidjeti što prolazi, a što ne
       - Saznajemo strukturu tablica, upita koje napadamo
     - Injekcija "na slijepo"
       - Koji izrazi su legitimni, a koji ne?
       - Učimo o bazi
     - Upit Union
       - Kombinacija upita kako bi dobili više podataka
       - SELECT column_name(s) FROM table1 UNION SELECT column_name(s) FROM table2;
   - Izbjegavanje napada umetanjem
     - Izbjeći interpretiranje naredaba
     - Koristiti pripremljene ili pohranjene procedure u SQL upitima
     - Validirati sve što korisnik upiše
     - Filteri

- Uvijek minimizirati ovlasti nad bazom podataka kako bi se spriječio pristup neželjenim podacima
- Ne prikazivati greške

2. Loša autentifikacija

- Cilj - pogoditi ime i lozinku korisnika ili ukrasti identifikator sjednice i lažno se predstaviti
- Podaci o sesiji ili korisniku moraju putovati u svakom zahtjevu
- Stanje se prati putem varijable SESSION ID (nalazi se u cookieu)
- Vrste
  - Brute force
    - Automatizirani alati
  - Lozinke iz rječnika
    - Slabe lozinke - qwert123, password123…
    - Ključna je duljina lozinke, ne nužno i kompleksnost
  - Vertikalni napadi
    - Cijeli rječnik za jednog korisnika
    - Tipično administrator
    - Pogađanje CMS-a i standardnog imena administratora
  - Horizontalni napadi
    - Jedna lozinka za sve korisnike
    - Kako pogoditi ime korisnika?
- Zaštita od pogađanja lozinke
  - CAPTCHA
  - Limit login attempts
  - Filtriranje po IP adresama i rasponima adresa
- Loše poruke o greškama
  - Ne javljati „Korisničko ime nije ispravno“
  - Javljati „Podaci za pristup su pogrešni“
- Dupliciranje lozinki
  - Korištenje istih podataka za prijavu na više web aplikacija
  - Provalom na jednoj web-aplikaciji napadač dobiva podatke za pristup drugim aplikacijama
- Identifikator sjednice (sessionID)
  - (Idealno) nasumičan niz znakova
    1. Poslužitelj ga generira nakon uspješne prijave korisnika
    2. Poslužitelj ga pohranjuje na svojoj strani
    3. Poslužitelj ga šalje korisniku
    4. Korisnik (preglednik) kod svakog sljedećeg zahtjeva na poslužitelj šalje dobiveni identifikator sjednice
  - Nekada kao parametar metode GET ili POST, danas najčešće u cookie-u
  - Alternativa/nadopuna identifikatorima sjednica - tokeni
    - kraće trajanje!
    - privremeni (access) i dugotrajniji (refresh) tokeni
  - Duljina barem 128 bitova
  - Sadržaj treba biti potpuno nasumičan i neovisan o korisniku
- Sigurni cookie

    - Zastavica HTTPOnly
    - Govori pregledniku da cookie-u može pristupiti isključivo poslužitelj kroz protokol HTTP
    - Ne smije mu pristupiti niti preglednik kroz javascript (sprečavamo krađu cookie-a putem XSS-a)
    - Dodatno osiguranje
        - Slati ih isključivo putem TLS-a (omogućiti zastavicu HTTPS only)
        - Odrediti domenu i putanju za koju vrijedi
        - Definirati vrijeme trajanja
- Izbjegavanje
    - Višefaktorska autentifikacija
    - Novi sessionID kod svakog zahtjeva -> tokeni
    - Dodatna autentifikacija kod osjetljivih akcija
    - Čuvanje lozinki - hash i SALT
    - Minimalne ovlasti po ulogama

3. Nesigurna pohrana osjetljivih podataka

- Ne identificiraju se svi osjetljivi podaci
- Napadači pristupe osjetljivim podacima i mijenjaju ih
- Problemi
    - Podaci se pohranjuju kao običan tekst
    - Podaci se prenose kao običan tekst
    - Korištenje zastarjelih algoritama za šifriranje
    - Korištenje slabih ključeva
    - Zaglavlja ne navode tip šifriranja podataka
- Rješenja
    - Verifikacija arhitekture
        - identificirati sve osjetljive podatke i mjesta na kojima se pohranjuju
    - Zaštita prikladnim mehanizmima
        - šifriranje podataka, baze podataka
    - Prikladna upotreba mehanizama zaštite
        - Koristiti snažne algoritme zaštite
    - Ne pohranjivati podatke koji nisu potrebni
    - Pratiti ranjivosti i nove preporuke za kriptoalgoritme i duljine ključeva

4. Vanjski XML entiteti (XXE)

- Potencijalno ranjive su aplikacije koje parsiraju XML datoteke
- Pogotovo ako se ne provjerava od kuda dolazi XML
- XML injection
    - Poslužitelj ili klijenti podatke šalju u XML-u
    - Manipuliranje podatcima
- Rješavanje problema
    - Izbjegavati korištenje složenijih XML struktura ako ne treba
    - Proučiti i ažurirati postavke XML parsera vezano uz učitavanje ili interpretiranja vanjskih entiteta

- Napraviti validaciju/sanitizaciju XML dokumenata prije parsiranja

5. Loša kontrola pristupa

- Kako se štiti pristup URL-ovima (stranicama)?
  - Ispravnom autorizacijom i sigurnim referencama na objekte
- Napadač krivotvori pristup stranicama kojima nema pristup
- Primjeri napada
  - Napadač vidi da URL naznačuje njegovu ulogu (user/getAccounts, mijenja u admin/getAccounts)
  - Napadač vidi da je njegov broj ?acct=6065 i mijenja ga u bliski broj
- Izbjegavanje
  - Izbjegavati reference
    - Zamjena s privremenim vrijednostima koje se na poslužitelju preslikavaju u prave
    - Provjeriti valjanost reference na objekt
  - Dopustiti pristup samo autentificiranim korisnicima
  - Provjeriti ovlasti za pristup i postupiti u skladu s njima
  - Verificirati arhitekturu
  - Verificirati implementaciju

6. Loše sigurnosne postavke

- Web-aplikacije očekuju da je sustav na kojem se nalaze siguran
- autentifikacijski podaci moraju se promijeniti u produkcijskoj verziji
- Učinci
  - Instalacija backdoor aplikacija ako OS ili APPserv nisu patchani
  - Nedostaci s iskorištavanjem XSS-a ako ne postoje patchevi za razvojni framework
  - Moguć pristup funkcionalnosti aplikacije zbog loše konfiguracije
- Primjeri
  - Ovlasti nad direktorijima
    - Omogućen je pregled direktorija u datoteci .htaccess
    - Napadač ima pregled strukture što mu olakšava napad ili preuzimanja datoteke i dekompajliranje
  - Wordpress
    - Tema koju koristite preporuča dodatak koji ima sigurnosne ranjivosti
    - Ili – dodaci nisu ažurirani na najnovije verzije
  - Komprimirana pohrana web-aplikacije na poslužitelju
    - Napadač je preuzima i analizira
- Izbjegavanje
  - Proces integracija i postavljanja aplikacije
  - Periodičko skeniranje i/ili audit
  - Puno toga se može postići kontrolom putem datoteke .htaccess
  - .htaccess - konfiguracijska datoteka za web poslužitelj (Apache)

7. Cross-site scripting (XSS)

- Same Origin Policy
    - Politika istog izvorišta
    - Odnosi se na kod koji se izvršava u pregledniku klijenta
    - Skripte koje se izvode na jednoj stranici smiju međusobno dijeliti pristup podacima
    - Problem - Sjedišta s više poddomena
    - Rješenje - Cross-Origin Resource Sharing
- Cross-site scripting (XSS) - podaci od napadača šalju se korisniku u preglednik
- Primjerice u javascriptu -> alert(document.cookie)
- Vrste
    - Reflektirani
        - XSS je dio URL-a i dovoljna je samo poveznica da se XSS izvede
        - Najjednostavniji i najčešći
        - Dobar je za preusmjeravanje i npr. krađu login podataka

```
//Probamo prolazi li XSS:
<script>alert('XSS test');</script>

//Možemo li preusmjeriti korisnika na drugu stranicu?
<script>document.location.href='http://www.hr';</script>

//Korisnicima šaljemo poveznicu s lažiranom stranicom – klasičan phishing s redirekcijom!
192.168.1.99/dvwa/vulnerabilities/xss_r/?name=<script>documen
t.location.href='http://www.hr';</script>
```

Slika 2 XSS Reflected

    - Pohranjeni
        - XSS se pohranjuje na poslužitelju (tipično kao unos forme)
        - Pohranjuje se u bazu
        - Svi korisnici koji posjete stranicu učitavaju XSS
- Zaštita
- Tipično se filtriraju <script> tagovi i znakovi
- Eliminacija uzroka
    - Ne uključivati ono što unese korisnik u izlaz aplikacije ili u povratni ispis
- Obrana
    - Prvo: kodirati sve što unese korisnik i izbjeći znakove <, >, {, } , “, ‘ i slične
    - Napraviti whitelisting onoga što korisnik može unijeti
- POST umjesto GET-a
- HTTPOnly Cookie-i

8. Nesigurna deserijalizacija

- Web aplikacije prenose i čuvaju podatke u serijaliziranom obliku
- Problem ako web aplikacija “vjeruje” serijaliziranom objektu i ne provjerava ga
- Izbjegavanje

- Ne vjerovati svemu što nam stiže od korisnika (preglednika) iako smo mi to poslali -> napadač je to mogao promijeniti!
- Isto vrijedi i za JS kod
- Koristiti JSON
- Potpisivati osjetljive podatke (digitalni potpis)
- Ne slati osjetljive podatke ako nije nužno
- Provjeravati očekivane tipove i dobivene tipove podataka

9. **Ranjive komponente**
   - Gotove komponente za različite namjene
   - Npr. Apache, NodeJS
   - Izbjegavanje
     - Identificirati korištene komponente
     - Provjeriti korištene komponente
     - Pratiti sigurnosne zakrpe i novootkrivene ranjivosti
     - Nadzor rada sustava i cjelokupne sigurnosti
     - Koristiti sigurnosne politike
     - Koristiti sigurnosne omotače – izolirati komponente i pratiti ulaz, izlaz

10. **Nedovoljan nadzor**
    - Većina napada podrazumijeva puno propalih pokušaja, “probe” poslužitelja i sličnih specifičnih radnji koje će u pravilu uzrokovati greške u dnevničkim zapisima
    - Moguće je prepoznati “vektore” napada i pretpostaviti na što napadači ciljaju
    - Rješenje
      - Log monitoring i alerting rješenja
        - Olakšati pregled dnevničkih zapisa administratorima
        - Obavijestiti ga o sumnjivim aktivnostima u stvarnom vremenu
      - Application Level Firewall
        - ”zna” prepoznati legitiman promet kod uobičajenih web aplikacija
        - ”zna” prepoznati maliciozan promet kod uobičajenih web aplikacija

Mrežna sigurnost 1.dio

<u>Komunikacijska sigurnost</u>

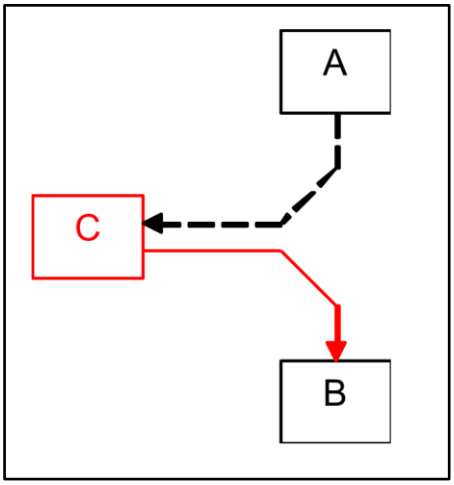
- Pretpostavljamo da moraju biti ispunjeni svi sigurnosni zahtjevi na podatke koji se razmjenjuju između A i B kako bi se te informacije smatrale sigurnima
- Svi zahtjevi su: tajnost, raspoloživost, cjelovitost, autentičnost i neporecivost
- **Presretanje, prisluškivanje**
  - Network Sniffing
  - Elektronička komunikacija se presreće i preuzima informacija
  - Postoji i zakonski regulirano presretanje (lawfull interception)

- Napadač postavlja svoju mrežnu karticu u promiskuitetni način rada - vidi sav promet na tom segmentu
- Mrežna kartica predaje sve pristigle pakete IP sloju
- Mnogi protokoli prenose autentifikacijske podatke u obliku čistog teksta -> username/password…
- Alati: Wireshark, tcpdump

- **Prekidanje, uskraćivanje**
  - Prekidanje - prekidanje normalnog tijeka komunikacije, usluge ili aplikacije
  - Uskraćivanje usluge - onemogućavanje usluge izazivanjem preopterećenja mreže ili umreženog sustava

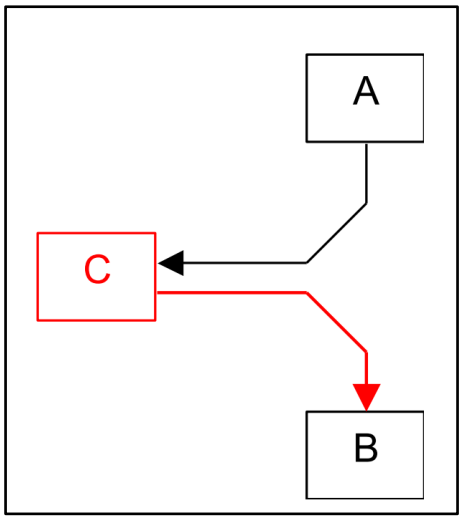
- **Promjena, kašnjenje**
  - Promjena - promjena ili uništenje informacije
  - Kašnjenje može izazvati isti učinak - podatak postaje nevažan

- **Umetanje, ponavljanje**
  - Umetanje, ubacivanje - ubacivanje zlonamjerne informacije
  - Ponavljanje - ubacivanje informacije prethodno preuzete presretanjem



Slika 3 Umetanje, ponavljanje

- **Lažno predstavljanje**
  - Maskiranje
  - Lažno predstavljanje
  - Preuzimanje identiteta i uloge korisnika
- **„Čovjek u sredini" (Man in the Middle)**
  - To je situacija u kojoj su prisutne sve prethodno spomenute prijetnje
  - Kako bi sve navedene prijetnje bile ostvarive napadač se mora nalaziti negdje na putu kojim se prenose podaci



Slika 4 MITM

Gdje se nalaze ranjivosti?

- Fizička ranjivost
- Ranjivosti u protokolima
- Ranjivosti u implementacijama
- Ranjivosti u konfiguraciji i korištenju
- Ranjivost koja je specifična za pojedinu okolinu

Ranjivosti protokola

- Dosta protokola Interneta je nastalo u vrijeme kada sigurnost nije bila visoko na listi prioriteta
- Primjeri ranjivih protokola: ARP, Ethernet, IP, TCP, UDP, niz aplikacijskih protokola

Protokol ARP

- ARP - protokol za pretvaranje 32 bitnih IP adresa u 48 bitne Ethernet (MAC) adrese
- Da bi računalo A poslalo poruku računalu B, mora znati njegovu MAC adresu
    - A šalje broadcast ARP zahtjev na mrežu (uključujući svoje preslikavanje)
    - B odgovara računalu A, porukom ARP odziv
    - preslikavanje se lokalno pohranjuje u svakom računalu u ARP
- ARP nema ugrađene mehanizme autentifikacije
- Moguće je poslati odgovor prije pravog računala te vratiti lažno preslikavanje adresa
- ARP poruke mogu se slati kontinuirano kako bi se (lažni) podaci zadržali u cacheu
- Cilj
    - Prisluškivanje prometa - switch prosljeđuje ethernet okvire između mrežnih sučelja na temelju ethernet adrese odredišta
    - Prekidanje - lažno preslikavanje IP adrese usmjeritelja na nepostojeću MAC adresu
    - DoS napad

    - Promjena
    - Ometanje
- Alati: arpoison, parasite
- Otkrivanje
    - Najjednostavniji način - ispis ARP cachea
    - Može se detektirati s nekog trećeg računala, na kojem se njuška mreža i traže lažni ARP odzivi
    - U slučaju DoS napada, lagano je ustanoviti da nešto nije u redu
- Zaštita
    - Ako postoji neobično ponašanje u mreži korisno je pogledati ARP cache
    - Korištenje hardvera koji će učiniti takve napade nemogućima ili više vidljivima (komutator)
    - onemogućavanje ARP-a i njegova ručna konfiguracija

Protokol IPv4

- Podaci koji se prenose nisu ni na koji način zaštićeni
- Laka izmjena pojedinih polja paketa
- Najčešće lažiranje izvorišnih IP adresa
- **IP zavaravanje (engl. IP spoofing)**
    - Slanje IP datagrama s lažnom adresom pošiljatelja
    - Najčešće se zloupotrebljava u DoS napadima
    - Rješenje
    - Filtriranje neispravnih izvorišnih adresa
    - Problem paketa s neispravnim izvorišnim adresama bi se djelomično riješio ispravnim podešavanjem usmjernika
- **IP fragmentacija**
    - Fragmentacija je obavezan dio IP protokola; kad je potrebno datagram podijeliti na manje dijelove prije učahurivanja u okvir podatkovne veze
    - Svaki fragment se dostavlja nezavisno
    - Može zavarati neke vatrozide i sustave za detekciju uljeza
    - Svi fragmenti imaju isti identifikacijski broj (IP ID)
    - Pomak (fragment offset) određuje smještaj fragmenta u sastavljenom datagramu
    - Zastavica “more fragments” postavljena je u svim fragmentima osim u zadnjem
    - Ping of Death
        - DoS napad koji prekoračuje maksimalnu veličinu IP datagrama
        - Kreira se i šalje fragmentirani IP datagram ukupne duljine veće od 65535 okteta
    - Teardrop
        - Napadač šalje dva fragmenta koji se djelomično prekrivaju “crash” kernela nakon sastavljanja fragmenata
    - TCP overwrite
        - varijacija napada Teardrop
        - IP datagram se fragmentira, TCP zaglavlje sadrži dozvoljeni port, na primjer 80, pa ga vatrozid propušta

        - neki sljedeći fragment ima „pomak” postavljen na 1 što znači da će port biti prepisan (npr. novi port će biti 23), sastavljeni paket preusmjerava se na novi port

Protokol ICMP

- DoS napadi
- Iskorištavanje tipa „ICMP redirect” za zlonamjerno preusmjeravanja prometa
- Uskraćivanje usluge slanjem lažiranih ICMP poruka o nedostižnom odredištu
- Implementacija prikrivenih kanala (engl. covert channel) korištenjem ICMP poruka
- Napad “smurf”
    - Započinje slanjem echo zahtjeva na sveodredišnu (“broadcast”) adresu posredničke mreže s lažiranom izvorišnom adresom jednakom adresi ciljne mreže (žrtve)
    - Računala u posredničkoj mreži odgovaraju slanjem echo odziva
    - Odgovori idu na adresu žrtve
    - Posrednička mreža i ciljna mreža zagušene prometom

Protokol DHCP

- Služi za automatsku dodjelu adresa i mrežnih parametara
    - Klijent šalje svima na mreži poruku DHCPDISCOVER
    - Poslužitelji odgovaraju klijentu s porukom DHCPOFFER
    - Klijent odabire poslužitelj i šalje svima DHCPREQUEST
    - Poslužitelj odgovara s DHCPACK
- Fiksiranje adresa na temelju MAC adrese radi kontrole pristupa
- Problemi
    - Nema nikakve zaštite poruka
    - Lažni DHCP poslužitelji na mreži
    - Bilo koji klijent može zatražiti parametre

Protokol IPv6

- Na razini RIR-ova IPv4 adrese su iscrpljene te je neminovno uvođenje IPv6
- Adrese su 128 bita
- Pojednostavljeno zaglavlje
- Fragmentacija se više ne provodi u mrežnom sloju
- Zaglavlje protokola IPv6 i dalje nema zaštite!
- Ranjivosti kojih više nema u IPv6
    - Skeniranje IPv6 mreža je otežano
    - Ne koriste se više broadcast adrese
    - Onemogućena je fragmentacija u usmjernicima
- Ranjivosti zajedničke protokolima IPv4 i IPv6
    - Skeniranje jedne adrese je i dalje moguće
    - Razrješavanje IP adresa u MAC adresu
    - Ne koristi se više ARP već ICMPv6, ali sve je ostalo isto

    - Protokoli ICMPv4 i ICMPv6 i dalje ranjivi
    - Protokol DHCP se i dalje koristi u obje mreže
    - Protokol IPsec se koristi za zaštitu oba protokola
- Ranjivosti specifične za protokol IPv6
    - Samostalno podešavanje IPv6 adrese
    - Problem velikog adresnog prostora
    - Višeodredišne adrese
    - Zloupotreba mehanizma DAD (Duplicate address detection) radi uskraćivanja usluge
    - Objava usmjerničkih podataka
    - Automatsko tuneliranje
    - Sigurnosni uređaji još nisu dovoljno sazreli

Protokol ICMPv6

- Vrlo značajan za ispravan rad protokola IPv6
- Posljedično, nije moguće filtrirati sav ICMPv6 promet

Poboljšanje sigurnosti na mrežnom sloju

- Protokol IP ne nudi nikakvu zaštitu
- Kriptiranje i zaštita integriteta
- VPN
- Za potpunu zaštitu preporučljivo je koristiti i (komplementarna) rješenja na višim slojevima - HTTPS/TLS

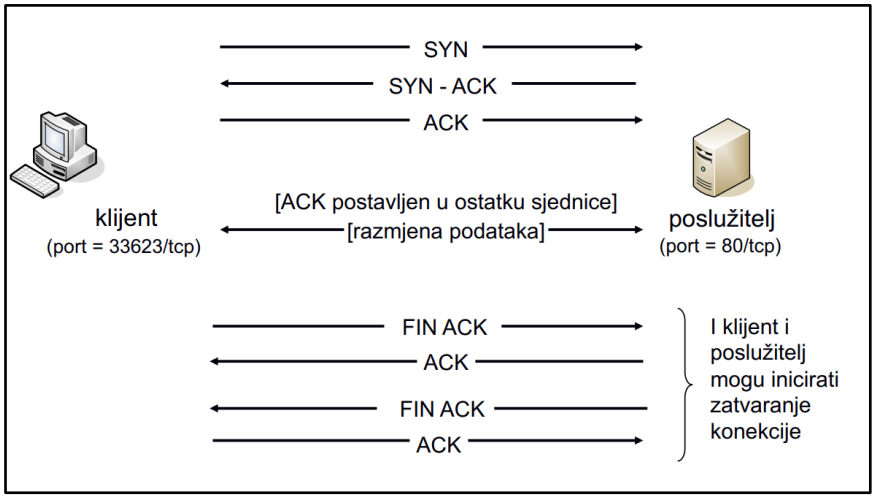
Protokol UDP

- Nespojni transportni protokol
- Nema ugrađene mehanizme za pouzdan prijenos
- Nema kontrole toka
- Duljina UDP zaglavlja: 8 okteta
- Napadi na UDP
- UDP obmana (UDP spoofing)
    - mijenjanjem izvorišne IP adrese predstavljamo se kao drugo računalo
    - IP adresa je jedini način identifikacije računala u protokolu UDP
    - Ne šalju se potvrde
- UDP otimanje (UDP hijacking)
    - napadač sluša vezu
    - odgovara na klijentov UDP zahtjev prije poslužitelja slanjem paketa s promijenjenom izvorišnim adresom
    - klijent misli da je primio paket od poslužitelja
- UDP oluje (UDP storms)
    - Jedan paket je dovoljan za pokretanje napada!
    - Obično se pošalje nekoliko paketa kako bi se pojačalo djelovanje
    - Petlja se izvodi dok jedno računalo ne završi

    - Koriste se echo (7), chargen (19), daytime (13), time (37)
- UDP reflection
    - Servisu koji koristi UDP (bez autentifikacije) pošalje se upit s lažiranom izvorišnom adresom a njegov odziv sadrži više podataka od upita
    - DNS amplification - 28 do 54 puta
    - NTP amplification - 556.9 puta

Protokol TCP

- Konekcijski (spojno) orijentirani transportni protokol
- Pouzdan, obostrana veza
- SEQ
    - Slijedni broj (“Sequence number”)
    - Označava redni broj prvog okteta koji se prenosi u korisničkim podacima
- ACK
    - Broj potvrde (“Acknowledgment number”)
    - Označava redni broj okteta koji pošiljatelj ove potvrde očekuje primiti
    - Ujedno potvrđuje da su svi podaci do tog okteta primljeni
- U paketu se šalje potvrda o zadnjim ispravno primljenim podacima
- Paket se prihvaća samo ako je unutar veličine predajnog prozora
- Za potvrdu se može koristiti i prazni segment
- Paketi sa zastavicama SYN ili FIN povećavaju slijedni broj iako ne sadrže podatke
- Za napad je bitan položaj napadača (za napad SYN flood nije!)
- Jedina potpuna zaštita je IPsec



Slika 5 Primjer TCP veze

- **Napad TCP SYN flood**
    - Poslužitelj po primitku SYN segmenta rezervira resurse
    - Veza je u poluotvorenom stanju koje traje neko vrijeme
    - Problem za napadača
        - Računalo koje primi SYN+ACK, a nije poslalo SYN, odgovara s RST
        - Napadač mora koristiti adresu s koje neće stići odgovor!
    - Ne postoji standardizirana niti potpuna zaštita

    - Neke metode zaštite su:
    - Povećanje broja dozvoljenih poluotvorenih veza
    - Skraćenje trajanja poluotvorene veze
    - Smanjenje količine stanja poluotvorene veze (SYN cache)
    - Zaštita uz pomoć kolačića (SYN cookies) - za inicijalni SYN se uopće ne čuva stanje
- RST napad
    - Slanje segmenta s postavljenom RST zastavicom
    - Problem je pogoditi parametre TCP veze
- FIN napad
    - Sličan RST napadu jedino se zatvara pojedini kraj veze

Mrežna sigurnost 2.dio

VPN

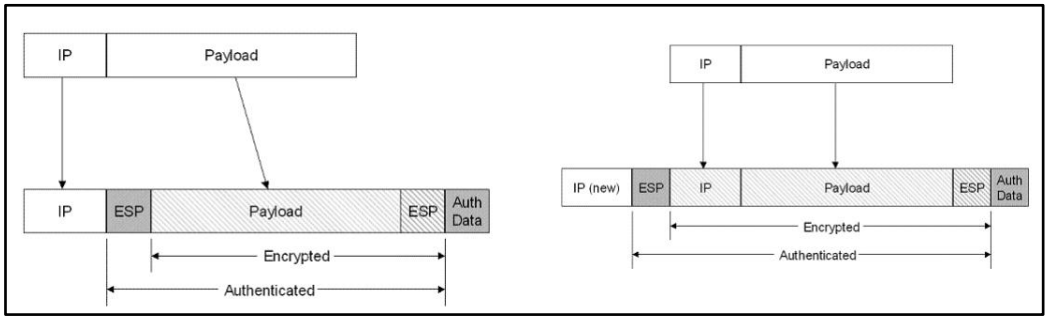
- Pojam koji označava stvaranje privatnih mreža nad javnom infrastrukturom Interneta
- Rješenja za ostvarenje virtualnih privatnih mreža
- OpenVPN, WireGuard, IPsec, Clientless VPN - TLS
- PTTP
    - Microsoft razvio 1999.
    - Na Internetu postoji usluga probijanja šifre za bilo koju PPTP konekciju unutar jednog dana - Ne koristiti!

- **Vrste VPN-a**
    - Od točke do točke (Site-to-site)
        - Između dva mrežna entiteta (na primjer usmjeritelja)
        - Privatne i zaštićene mreže iza oba entiteta
    - udaljeni pristup (Remote Access)
        - Između uređaja i usmjeritelja
        - Na udaljenoj lokaciji se ne nalazi zaštićena mreža

- **IPSec**
    - Služi za povezivanje dviju ili više mreža (VPN), povezivanje osobnih računala na korporativnu mrežu, povezivanje dva računala međusobno
    - Autentifikacija putem certifikata, dijeljene tajne ili EAP-a
    - Protokol definira ponašanje krajnjih točaka i protokole za razmjenu upravljačkih informacija i podataka
    - Ponašanje krajnjih točaka definirano bazama SPD i SAD
    - SPD (Security Policy Database) definira što se treba zaštititi
        - Navodi što treba učiniti s paketom koji odgovara
    - SAD (Security Association Database) definira kako treba štiti
        - Sadrži odabrane kriptografske algoritme i ključeve

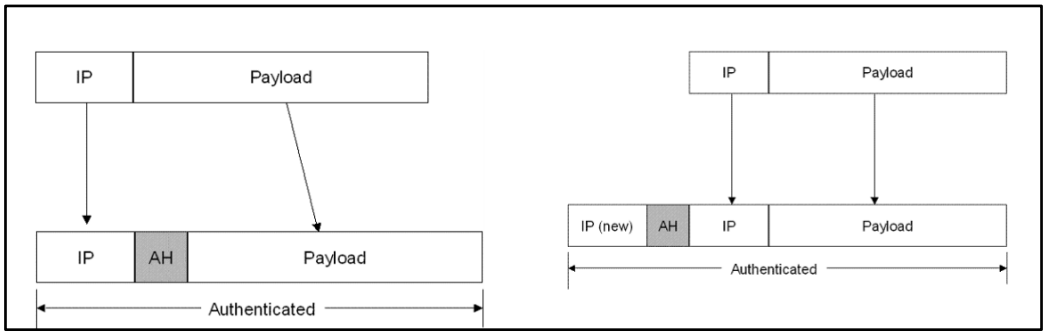
- Osnovni protokoli: ESP (Zaštita tajnost, integriteta i autentičnosti), AH (Zaštita integriteta i autentičnosti), IKE (Uspostava ključeva)

- **Protokol ESP**
  - Struktura zaglavlja paketa ESP (Encapsulating Security Payload) u prijenosnom (lijevo) i tunelirajućem (desno) načinu rada



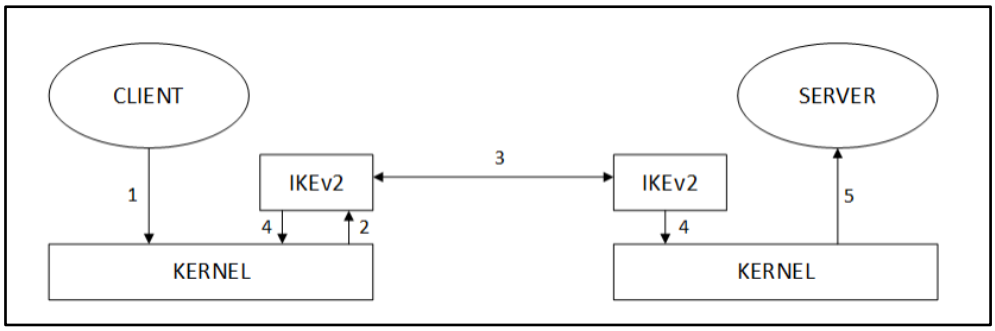
Slika 6 Protokol ESP

- **Protokol AH**
  - Struktura zaglavlja paketa AH (Authentication Header) u prijenosnom (lijevo) i tunelirajućem (desno) načinu rada



Slika 7 Protokol AH

- **Protokol IKEv1 i IKEv2**
  - Zadaće protokola su
    - Autentifikacija partnera
    - Dogovor oko sigurnosnih asocijacija
    - Periodička razmjena ključeva
  - Razlike IKEv2 u odnosu na IKEv1
    - IKEv2 pojednostavljen
    - Potrebno je manje razmjena paketa kako bi se uspostavila prva sigurnosna asocijacija
    - Uklonjena i jedna ranjivost u posebnom načinu rada

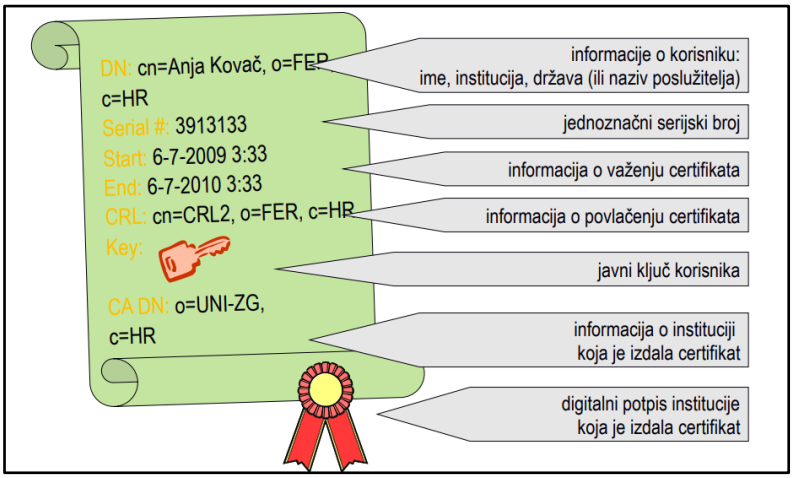


Slika 8 Primjer rada protokola IKE i ESP/AH

- **Nekriptirani VPN sustavi**
  - Ponekad se pod nazivom VPN-a nudi neka nezaštićena usluga
  - MPLS je tehnologija slična na ATM-u koja IP adrese mijenja labelama
  - U toj usluzi nema nikakvog kriptiranja te je IPsec ili sličan mehanizam i dalje nužan

Digitalni certifikati

- Certifikat – digitalni objekt
- Sadrži javni ključ i ostale informacije o subjektu, izdavatelju i valjanosti
- Certifikat izdaje i digitalno potpisuje izdavatelj certifikata



Slika 9 Sadržaj osobnog certifikata

- **CA certifikati**
  - Certifikati svih poznatih izdavatelja ugrađeni su u preglednike ili operacijski sustav
  - Unutar organizacije je moguće kreirati vlastito certifikacijsko tijelo koje izdaje samopotpisani certifikat
  - Datoteke certifikata
    - .CER/.CRT/.DER – binarni, DER kodirani certifikat
    - .PEM – dodatno kodiran po Base64
    - .PFX - PKCS#12, javni i privatni ključ (zaštićen lozinkom)

- Valjanost certifikata
  - Polja u certifikatu: „not valid before" i „not valid after"
  - Za vrijeme roka valjanosti certifikat može biti opozvan

Protokol TLS

- Protokol TLS služi za zaštitu komunikacije
- **Model prijetnje**
  - Krajnje točke komunikacije su sigurne
  - Ostali sustavi mogu biti pod kontrolom napadača
  - Napadač ima potpunu kontrolu nad komunikacijskim kanalom
  - Eksplicitno ne brinemo o napadima uskraćivanja usluge
- **Najčešća upotreba TLS-a: HTTPS**
  - Korisnik na klijentskoj strani (u pregledniku) zahtijeva dokument s URL koji sadrži https umjesto http
  - Preglednik prepoznaje SSL/TLS zahtjev i uspostavlja konekciju s poslužiteljem na TCP portu 443
- **Osnovna funkcionalnost protokola** - potvrda identiteta poslužitelja i zaštita tajnosti i autentičnosti komunikacije
- Izvršava se nad protokolom TCP
- Protokol također omogućava autentifikaciju klijenta korištenjem certifikata
- **Presretanje protokola**
  - Za tvrtke je kriptirani mrežni promet problematičan
  - Narušavanje politika i pravila korištenja intraneta i Interneta, skidanje zloćudnog koda
  - U slučaju presretanja komunikacije zaštićene TLS-om klijenti dobivaju upozorenje
- Napadi na protokol – Heartbleed, BEAST, POODLE
- **TLS 1.3**
  - TLS 1.3 je brži i sigurniji protokol od verzije 1.2
  - Uklonjene su zastarjele i nesigurne komponente protokola
- **Preporuke za korištenje TLS protokola**
  - Koristiti ključeve od minimalno 2048 bita za RSA ili 256 bita za ECDSA
  - Samostalno generirati privatni ključ na sigurnom računalu
  - Izbjegavati slabe algoritme kao što je RC4
  - Onemogućiti kompresiju, pregovaranje koje inicira klijent

Napadi uskraćivanja usluge (DoS/DDoS)

- Nisu specifični za mrežni sloj
- Obrana vrlo teška i ovisi o konkretnom napadu i specifičnostima samog napada
- **Vrste mrežnih (D)DoS napada**
  - Napadi preplavljivanja (Lažirani i legitimni UDP promet, ICMP i DNS preplavljivanje)
  - Preplavljivanje koje iskorištava karakteristike protokola (TCP SYN preplavljivanje, RST/FIN preplavljivanje)
  - Reflektirajući napadi preplavljivanja (Smurf attack)
  - Napadi preplavljivanja s pojačanjem (DNS amplification, NTP amplification)

- **Vrste aplikacijskih (D)DoS napada**
    - Reflektirajući/amplifikacijski napadi (vrlo slični mrežnim DDoS napadima, ali ciljaju protokole viših slojeva)
    - HTTP napadi (Slow request/response attacks, asimetrični napadi)
- **Zaštita**
    - Zaštita na strani žrtve
        - Zaštita od napada vrlo specifična o konkretnoj situaciji
        - Npr. ako je napad temeljen na UDP-u moguće je blokirati UDP
    - Zaštita na komunikacijskom putu do žrtve (suradnja s ISP-om)
    - Djelovanje na strani napadača i C&C poslužitelja

Mrežna sigurnost 3.dio

Aplikacijski sloj

- Poslužiteljske aplikacije osluškuju zahtjeve na dobro poznatim pristupima
- Administrator (ili običan korisnik) na nekom računalu korištenjem odgovarajućih alata može dobiti popis:
    - Pristupa na kojima čeka neka aplikacija
    - Poslužiteljskih aplikacija koje osluškuju zahtjeve
    - Statusa veza
- Jedan od alata koji daje te informacije je netstat
- **Udaljeno otkrivanje aplikacija**
    - Temeljni način udaljenog otkrivanja aplikacija je skeniranje pristupa kako bi se utvrdilo koji su otvoreni
    - Otvoren pristup znači da je neka aplikacija prisutna
    - Potrebno je dodatno prikupljanje informacija kako bi napadač otkrio aplikaciju, i njenu verziju
- **Otkrivanje aktivnih TCP aplikacija**
    - Pokušaj uspostave veze (najjednostavnija metoda koja uspostavlja u potpunosti vezu te ju odmah prekida)
    - TCP SYN skeniranje (šalje se SYN te gleda odgovor)
    - U oba slučaja, ako nema odgovora tada negdje na putu postoji nekakav filter i ne znamo kakva je situacija
    - TCP FIN skeniranje (šalje se segment s FIN zastavicom. U slučaju da nema ničega na pristupu, vraća se RST, u suprotnom se zahtjev ignorira)
    - Skeniranje s fragmentacijom (Nije posebna vrsta skeniranja već mehanizam izbjegavanja detekcije)
- **Skeniranje UDP porta**
    - Slanje (praznog) UDP datagrama
    - Za zatvoren pristup pristižu poruke “ICMP port unreachable”
    - Kada je pristup otvoren ne šalje se nikakav odgovor
    - Potencijalni problemi za napadača
        - UDP je nepouzdan te je potrebno pokušati nekoliko puta kako bi bili sigurni da nije došlo do gubitaka
    - Vrlo spora tehnika skeniranja

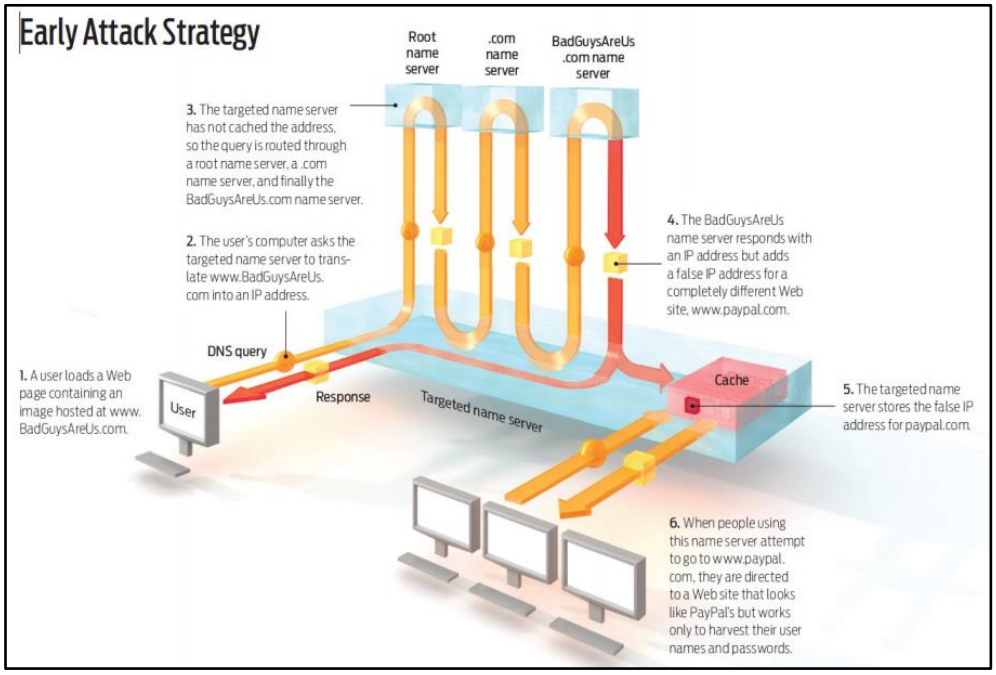
- **Poteškoće sa skeniranjem za napadača**
  - Relativno velik broj pristupa po čvoru
  - Potencijalno velik broj čvorova koje je potrebno skenirati
  - Ako je neki port otvoren ne znači da se tamo nalazi očekivana aplikacija
- **Detekcija aplikacije**
  - Napadač se spaja na port
  - Koristeći očekivani protokol pokušava komunicirati s aplikacijom
  - Problemi za napadača
    - Ako aplikacija ne objavljuje svoju verziju/tip ili objavljuje neku generičku ili lažnu verziju
    - Na aplikacije se stavlja zakrpa koja ne mijenja prijavljenu verziju aplikacije
- **Otkrivanje vrste i verzije operacijskog sustava**
  - Detekcija OS-a temelji se snimanju ponašanja njegova mrežnog stoga te usporedbi s bazom poznatih operacijskih sustava
  - Detekcija nije u potpunosti pouzdana, tj. uvijek postoji mogućnost pogreške
- **Napadi pogađanja grubom silom**
  - Pokušaj otkrivanja nepoznate ili tajne informacije upotrebom pogađanja
  - Sve usluge koje omogućavaju prijavu putem mreže ranjive su na pogađanje
  - Napad pogađanja može biti:
    - „on-line" uključuje interakciju s uslugom
    - „off-line" radi na ukradenim podacima
  - Zaštita
    - Ograničavanje pristupa usluzi
    - Kvalitetne, jake lozinke (dobra entropija!)
    - Ograničavanje broja pokušaja, zaključavanje
    - 2FA
    - Pohrana lozinki u šifriranom obliku ili u obliku sažetka
- **Poslužitelji elektroničke pošte**
  - Elektronička pošta koristi barem dva poslužitelja
    - MTA - Mail Transfer Agent
    - MUA - Mail User Agent
  - Danas je uobičajeno integrirano rješenje (tzv. groupware)
  - Poslužitelj elektroničke pošte direktno izložen na Internetu
  - Obavezna redovita nadogradnja
- **Usluga prijenosa datoteka**
  - Originalno za tu namjenu bio je predviđen protokol FTP (File Transfer Protocol)
  - Nema zaštitu komunikacije, prijenos lozinke preko mreže
  - Protokol uključuje otvaranje zasebnih TCP veza!
  - Povećava kompleksnost uređaja vatrozid/NAT
  - Preporuka: izbjegavati i koristiti alternativu SFTP/SCP
- **Udaljeni rad**
  - Najpoznatiji protokol: SSH
  - SSH Transport Layer Protocol
    - Dogovara način razmjene ključeva, asimetrični algoritam šifriranja, simetrični algoritam šifriranja, algoritam za autentifikaciju poruka i algoritam kriptografskog sažetka
    - Autentifikacija poslužitelja korištenjem para ključeva (javni/privatni)

        - Prilikom prvog spajanja klijentski program korisniku prikazuje sažetak poslužiteljskog ključa
    - Usluge temeljene na protokolu SSH
        - Udaljen rad (ssh klijent)
        - Prijenos datoteka (SFTP i SCP klijenti)
        - Tuneliranje Ethernet okvira ili IP datagrama
        - Prosljeđivanje lokalnih i udaljenih pristupa
    - Mogući problemi sa SSH
        - Korisnik nije zaštitio tajni ključ lozinkom
        - Popis računala i javnih ključeva
        - Zamjena i povlačenje ključeva je zahtjevna

DNS

- **Svrha napada na sustav DNS**
    - Sprečavanje pristup određenoj usluzi
    - MITM napad ili podmetanje lažnih sjedišta
    - Preuzimanje domena
- **Prijetnje sustavu DNS**
    - Presretanje paketa (MITM)
    - Primjena IPsec/TLS i sličnih rješenja nije odgovarajuća (štiti samo pojedine korake, ne s kraja na kraj)
    - Pogađanje ID vrijednosti i predviđanje upita
        - Napadač nije na putu i mora pogoditi ID u paketu te izvorišni pristup
    - Name chaining
        - Podskup napada trovanja priručne memorije (engl. cache poisoning)
        - U odgovoru se šalje informacija koja uzrokuje da žrtva šalje DNS upit prema napadačevom poslužitelju
        - Djelomična zaštita sprečavanja trovanja priručne memorije je provjera relevantnosti dobivenih informacija s obzirom na poslani upit
    - Manipulacija upotrebom poslužiteljima
        - Klijent vjeruje nekom poslužitelju koji je pod kontrolom napadača
    - Uskraćivanje usluge
        - Rješava se višestrukim DNS poslužiteljima po domeni razmještenima u različitim mrežama
        - Ponekad rješava se upotrebom ANYCAST adresa
- **Zaštita sustava DNS**
    - Zaštita od DNS Cache Poisoning
        - TXID (16 bita) + random source port (16 bita)
    - Mehanizam TSIG
        - Temelji se na dijeljenom ključu uz pomoć kojega se generira potpis
        - Koristi se za dinamička osvježavanja zone te za prijenos zone na sekundarne poslužitelje
    - DNSSEC
        - Osigurava kriptografski dokaz ispravnosti primljenih podataka

- Klijenti korištenjem resolvera koji provjeravaju valjanost dobivaju zajamčeno sigurne podatke
- Za podatke koje ne može provjeriti resolver vraća SERVFAIL
- Za zaštitu se koristi asimetrična kriptografija
- Podaci, zapisi na poslužitelju (RR – Resource Records), potpisuju se privatnim ključem
- Potpisom se osigurava valjanost zapisa s kraja na kraj -> između autoritativnog poslužitelja i resolvera
- Možemo li tim podacima vjerovati? -> Da ako je root (".") potpisan!
- **Problemi sustava DNSSEC**
    - DNSSEC ne osigurava povjerljivost podataka
    - DNSSEC ne štiti od DDoS napada
    - Utjecaj na mrežu i vatrozide

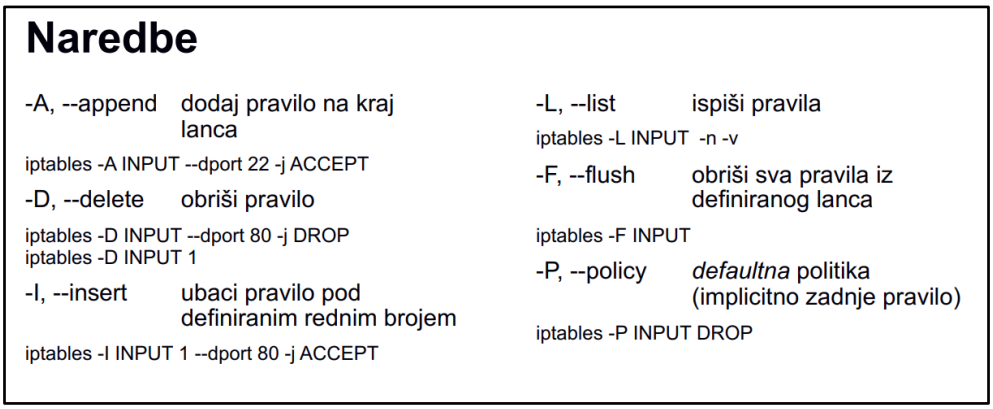


Slika 10 DNS cache poisoning

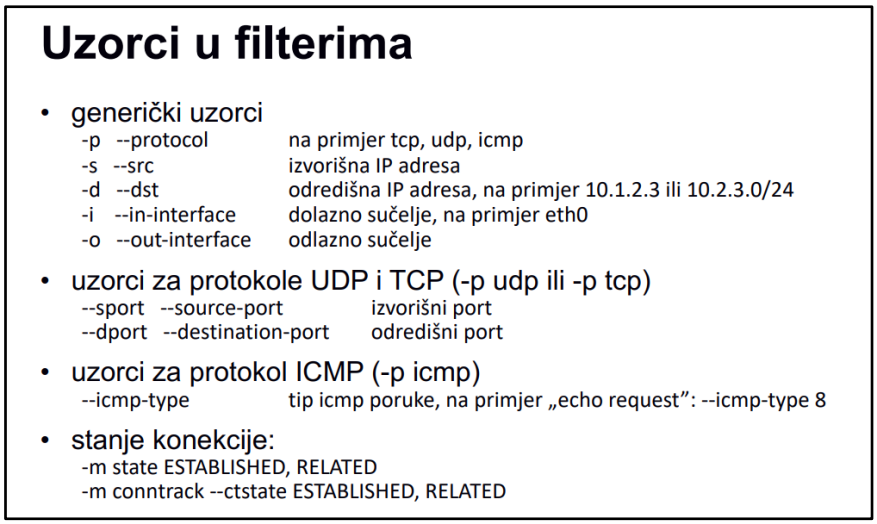
Vatrozid

- Uređaj koji radi na mrežnom sloju
- Smješten između dvije ili više mreža
- **Princip rada**
    - Provodi sigurnosnu politiku kontrolom pristupa
    - Svaki paket koji prolazi provjerava se sa bazom pravila koja određuje što treba učiniti s paketom
- **Elementi arhitektura mreža s vatrozidom**
    - Segmentacija mreže na razne razine povjerljivosti
    - Demilitarizirana zona (DMZ)
    - Perimetar – granica mreže (danas nije toliko jasan!)
    - Konfiguracije s jednim i dva vatrozida

- **NAT**
  - Zasebna funkcionalnost, često integrirana s vatrozidom, nije za sigurnost
- Poslužiteljska mreža može biti zaštićena dodatnim vatrozidom
- Poslužitelji kojima se pristupa iz Interneta smještaju se u posebnu mrežu: Demilitarizirana zona (DMZ)
- **Primjeri vatrozida**
- **Netfilter / iptables**
  - iptables se koristi za postavljanje, održavanje i provjeru pravila IP vatrozida ugrađenog u Linux kernel
  - pravila su organizirana u lance
- **Packet filter**
  - Packet filter usmjerava i filtrira pakete između unutarnjih i vanjskih sučelja
  - Selektivno propušta ili blokira određene tipove paketa na temelju:
    - Protokola
    - IP adresa izvora / odredišta
    - TCP zastavica
    - TCP ili UDP izvorišni/odredišni port
  - Prednosti - jednostavna implementacija i dobre performanse
  - Ograničenja - ograničena provjera, složena konfiguracija, nije dovoljno fleksibilno i proširivo
- **Statefull Inspection**
  - Radi kao paket filter (pristupne liste) + održavanje stanja
  - Dohvaća i informacije iz protokola na višim slojevima
  - Provjera svakog paketa
- **Iptables chains**
  - Vrste
    - input - ulazni
    - output - izlazni
    - forward - prosljeđivački
    - prerouting, postrouting, korisnički specificirani lanci, masquerading, port forwarding
  - Lanac se sastoji od niza pravila koja se obrađuju slijedno
  - Obrada završava ako se „skače" na lance: ACCEPT – paket se prihvaća, DROP – paket se odbacuje, REJECT – kao DROP ali šalje ICMP poruku ili TCP reset



Slika 11 Iptables naredbe



Slika 12 Iptables uzorci u filterima

- Vatrozid nije rješenje svih problema sigurnosti
- **Posrednički poslužitelji**
  - Vatrozid radi na 3. sloju ISO/OSI RM-a (i 4. sloju)
  - Posrednički poslužitelji omogućavaju bolji nadzor mrežnog prometa
  - ALI: Bez vatrozida nije moguće dosljedno provoditi politiku korištenja posredničkog poslužitelja

IDS

- Sustavi za detekciju upada (Intrusion Detection Systems)
- Temelje se na ideji da se praćenjem ponašanja sustava ili prometa na mreži može detektirati incident
- **Podjele prema načinu rada**
  - Bazirane na pravilima
  - Na detekciji ponašanja ili anomalijama
- **Podjele prema mjestu nadzora**
  - Mrežni (NIDS) – uzimaju podatke s mreže
  - Računalni sustavi (HIDS) – uzimaju podatke s računala
- Mrežni sustavi
  - Postavljaju se na neke ključne točke na kojima snimaju promet
  - Problem je i šifrirana komunikacija
- **Sustavi za prevenciju upada (Intrusion Prevention Systems)**
  - Osim detekcije rade i prevenciju
  - Prevencija može biti postavljanje dodatnih pravila na vatrozidu
  - Ako nisu dobro podešeni mogu onemogućiti ispravan rad mreže
- **Otkrivanje ranjivosti u mreži**
  - Otkrivanje ranjivosti može se obaviti na dva temelja načina:
    - Skeniranje mrežnih raspona
    - Penetracijska ispitivanja

Mrežna sigurnost 4.dio

Sigurnost bežičnih mreža

- Bežične mreže koriste elektromagnetske valove za prijenos podataka
- Mogu biti 802.11, mobilne mreže, Bluetooth
- Dva osnovna načina rada 802.11:
  - Ad-hoc - omogućava direktnu komunikaciju stanica
  - Infrastrukturni - koristi se pristupna točka (AP) preko koje svi komuniciraju
- **Protokoli za sigurnost bežičnih mreža**
  - Za sigurnost bežičnih mreža definirani su WEP, WPA, WPA2 i WPA3
  - WEP - primjer kako ne upotrebljavati kriptografiju
  - WPA - uveden kao privremena mjera, baziran na draftu 802.11i specifikacije
  - WPA2 definiran 2004. godine
  - WPA3 definiran 2018. godine - poboljšana zaštita prilikom korištenja nedovoljno kompleksnih lozinki, uklonjeni kripto algoritmi koji se smatraju nesigurnima, uvedena zaštita upravljačkih okvira
- **Kontrola pristupa bežičnoj mreži**
  - WPA/WPA2/WPA3 PSK (pre-shared key, dijeljena tajna)
    - Jednostavno postavljanje
    - Efektivno se radi o lozinci što znači da se mogu provoditi napadi koji se provode na njih
  - WPA/WPA2/WPA3 Enterprise
    - Centralizirana autentifikacija koju obavlja poseban poslužitelj
- **Fizički sloj**
  - Na fizičkom sloju definiraju se radio karakteristike
  - Koristi se nelicencirani spektar centriran na 2.4 GHz i 5 GHz
  - Oblikom i razmještajem antena te snagom može se utjecati na pokrivenost
- **Vrste okvira i njihova zaštita**
  - U 802.11 bežičnim mrežama upotrebljavaju se tri vrste okvira
    - Podatkovni okviri - prenose korisničke podatke
    - Upravljački okvir - upravljanje MAC-om
    - Kontrolni okviri - upravljanje pristupom mediju
  - Samo podatkovni okviri su kriptografski zaštićeni
- **Napadi uskraćivanjem usluge**
  - RF ometanje
  - Virtualno ometanje
  - Lažiran zahtjev za odspajanjem
  - Connection request flooding
- **Napadi na kriptografiju**
  - WEP - uz pomoć gotovih alata vrlo jednostavno je moguće doći do dijeljene tajne
  - WPA ima određenih problema - korišteni algoritam za zaštitu integriteta nije dovoljno jak te je u prosjeku nakon 2^{28} pokušaja moguće lažirati sadržaj poruke
  - WPA2 ima ranjivost KRACK
- **Nekriptografski napadi na WPA i WPA2**
  - WPA PSK ranjiv na pogađanje dijeljene tajne
  - PSK je moguće otkriti i kompromitiranjem klijenata

    - PSK omogućava spajanje na mrežu, ali ne i dešifriranje snimljenog prometa
- **Napad na sustav WPS**
    - WPS (engl. Wi-Fi Protected Setup) napravljen kako bi se olakšalo podešavanje WPA PSK zaštite
        - Korisnik na računalu ukuca 8-znamenkasti PIN zapisan na kućnom usmjerniku
        - Usmjernik pošalje dobru dijeljenu tajnu računalu i na dalje se upotrebljava WPA PSK
    - Problem
        - Radi se o samo 8 znamenkastom broju, a zadnja znamenka je kontrolna
        - Znamenke se prenose u grupama 4+3, pri čemu AP daje odgovor već nakon prve grupe
        - Dakle, potrebno je samo 11000 (104+103) pokušaja (od početnih 108!)
- **Neovlaštene i otvorene pristupne točke**
    - Neovlaštene pristupne točke (engl. Rogue access points)
        - Pristupne točke dolaze u raznim formama – postoje USB verzije koje se mogu priključiti na prijenosna/stolna računala
        - Napadač koji se pokušava ubaciW u komunikaciju ili dohvaWW inicijalnu razmjenu radi vjerodajnica
    - Otvorene pristupne točke na javnim mjestima ili u kafićima
        - Problematične jer mogu biti namjerno podmetnute
        - Ako nisu podmetnute, na tim otvorenim mrežama može se nalaziti napadač vrebajući žrtve