Sigurnost računalnih sustava

Mrežna sigurnost

- treći dio (aplikacije, vatrozid, IDS)

doc. dr. sc. Ante Đerek
doc. dr. sc. Stjepan Groš
izv. prof. dr. sc. Miljenko Mikuc
izv. prof. dr. sc. Marin Vuković

Aplikacijski sloj

Vidljivost aplikacija na mrežnom čvoru (1)

- Poslužiteljske aplikacije osluškuju zahtjeve na dobro poznatim pristupima
  - Pristupi su brojevi od 1 do 65535 (za svaki prijenosni protokol: TCP, UDP, SCTP, …)
- Administrator (ili običan korisnik) na nekom računalu korištenjem odgovarajućih alata može dobiti popis:
  - Pristupa na kojima čeka neka aplikacija
  - Poslužiteljskih aplikacija koje osluškuju zahtjeve
  - Popis statusa veza (uspostavljene ili bilo koje drugo stanje)
- Na Unix / Linux / Windows OS-u alat je netstat
  - Ima i mnoštvo drugih sa i bez grafičkog sučelja

Vidljivost aplikacija na mrežnom čvoru (2)

- Primjer (izvršavanje na Linuxu)

```
$ netstat -an4
Active Internet connections (servers and established)
Proto Recv-Q Send-Q   Local Address           Foreign Address         State
tcp        0      0   0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0   127.0.0.1:38245         0.0.0.0:*               LISTEN
tcp        0    172   31.147.204.44:22        161.53.19.9:61407       ESTABLISHED
tcp        0      0   31.147.204.44:22        95.168.116.4:43619      ESTABLISHED
udp        0      0   0.0.0.0:5555            0.0.0.0:*
```

Udaljeno otkrivanje aplikacija

- Temeljni način udaljenog otkrivanja aplikacija je skeniranje pristupa kako bi se utvrdilo koji su otvoreni
  - Najjednostavnija metoda skeniranja je pokušaj pristupa aplikaciji
  - Može se obaviti aplikacijom (Web preglednik u slučaju Weba) ili, općenitije, NetCat / telnet aplikacijom u slučaju protokola TCP
- Otvoren pristup znači da je neka aplikacija prisutna
  - Samo na temelju te informacije se ne može znati koja aplikacija je prisutna.
- Potrebno je dodatno prikupljanje informacija kako bi napadač otkrio aplikaciju, i njenu verziju
  - Točna verzija je potrebna radi pronalaženja potencijalnih ranjivosti

Otkrivanje aktivnih TCP aplikacija (1)

- Pokušaj uspostave veze (engl. TCP connect)
  - Najjednostavnija metoda koja uspostavlja u potpunosti vezu te ju odmah prekida
  - Moguće korištenje specifičnih alata ili generičke NetCat/telnet naredbe
  - Upostava veze -> postoji aplikacija na pristupu, RST ne postoji
- TCP SYN skeniranje
  - tzv. poluotvoreno skeniranje (engl. half-open scanning)
  - Šalje se SYN te gleda odgovor
    - SYN+ACK znači da aplikacija sluša, čeka uspostavu veze na danom pristupu
    - RST znači da na danom pristupu ne čeka nikakva aplikacija
- U oba slučaja, ako nema odgovora tada negdje na putu postoji nekakav filter i ne znamo kakva je situacija

Otkrivanje aktivnih TCP aplikacija (2)

- TCP FIN skeniranje
  - Šalje se segment s FIN zastavicom. U slučaju da nema ničega na pristupu, vraća se RST, u suprotnom se zahtjev ignorira
  - Određene implementacije u oba slučaja šalju RST segment
  - Sigurno možemo znati samo da nema ničega na pristupu
- Skeniranje s fragmentacijom (engl. fragmentation scanning)
  - Nije posebna vrsta skeniranja već mehanizam izbjegavanja detekcije
  - Fragmentiranjem IP paketa u kojemu je TCP segment otežava se detekcija skeniranja

Skeniranje UDP porta (1)

- Slanje (praznog) UDP datagrama
- Za zatvoren pristup pristižu poruke “ICMP port unreachable”
  - Osim ako je negdje na putu instaliran filter
- Kada je pristup otvoren ne šalje se nikakav odgovor
  - Pod pretpostavkom da poslužitelj ignorira poruke koje nisu ispravno formatirane i nisu primljene u ispravnom redoslijedu
  - Ako se ne dobije ICMP poruka pretpostavlja se da je port otvoren
    - Što baš ne mora biti slučaj…

Skeniranje UDP porta (2)

- Potencijalni problemi za napadača
  - UDP je nepouzdan te je potrebno pokušati nekoliko puta kako bi bili sigurni da nije došlo do gubitaka (posljedica je također da nema odgovora!)
  - Neki operacijski sustavi ograničavaju brzinu slanja ICMP poruka (RFC 1812, 4.3.2.8)
    - Generiraju ograničen broj ICMP poruka u sekundi
- Vrlo spora tehnika skeniranja

Poteškoće sa skeniranjem za napadača

- Relativno velik broj pristupa po čvoru
  - Mora balansirati brzinu i detaljnost kako bi izbjegao otkrivanje
  - Skeniranje samo određenog podskupa pristupa
- Potencijalno velik broj čvorova koje je potrebno skenirati
  - 254 u slučaju mreže s mrežnom maskom 24
- Ako je između cilja i napadača filter ne vraćaju se odgovori i nije moguće znati je li port otvoren ili ne
- Ako je neki port otvoren ne znači da se tamo nalazi očekivana aplikacija

Detekcija aplikacija i operacijskog sustava

- Kako bi napadač mogao iskoristiti aplikaciju koja sluša na nekom pristupu mora znati koje ranjivosti ima
  - Poznavanjem točne verzije aplikacije i koristeći baze ranjivosti može pripremiti napad na aplikaciju
  - Slično vrijedi i ako traži novu ranjivost
  - Određene aplikacije izvršavaju se na više operacijskih sustava pa je dobro znati i koji je operacijski sustav korišten
- Napad je moguć i na operacijski sustav, za što je potrebno također znati točnu verziju operacijskog sustava
  - „OS fingerprinting”

Detekcija aplikacije

- Napadač se spaja na port
  - Neke aplikacije objavljuju svoju verziju u pozdravnim porukama koje šalju odmah po spajanju
  - Koristeći očekivani protokol pokušava komunicirati s aplikacijom
    - Na taj način utvrđuje da pretpostavljena aplikacija čeka na pristupu
  - Moguće je na temelju konverzacije s aplikacijom utvrditi verziju
- Problemi za napadača
  - Ako aplikacija ne objavljuje svoju verziju/tip ili objavljuje neku generičku ili lažnu verziju
  - Na aplikacije se stavljaju zakrpe (patch) koje ne mijenjaju prijavljenu verziju aplikacije
  - Funkcionalnosti iz novijih verzija se dodaju na starije (a s njima i ranjivosti) pri čemu se također ne mijenja prijavljena verzija

Otkrivanje vrste i verzije operacijskog sustava

- Norme i specifikacije protokola ne definiraju apsolutno svaki detalj ponašanja implementacije
  - Kada se implementira protokol odabire se različita ponašanja – slučajno ili namjerno
  - Iz verzije u verziju također se nadograđuje mrežni stog te mu se mijenja ponašanje
- 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
  - snimljenom ponašanju odgovara više operacijskih sustava!

Primjer alati za skeniranje: nmap

```
# nmap -O 31.147.204.44
Host is up (0.0011s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.4

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.93 seconds
```

Napadi pogađanja grubom silom

- Pokušaj otkrivanja nepoznate ili tajne informacije upotrebom pogađanja (engl. brute force)
  - Najčešće se pogađaju lozinke
  - Pogađanje korisničkih imena, dijeljenih tajni,…
- Sve usluge (engl. services) koje omogućavaju prijavu putem mreže ranjive su na pogađanje
  - telnet, ftp, r* naredbe, ssh, http, snmp, …
- Napad pogađanja može biti „on-line” ili „off-line”
  - „on-line” uključuje interakciju s uslugom
  - „off-line” radi na ukradenim podacima

Zaštite od pogađanja grubom silom

- Ograničavanje pristupa usluzi
- Kvalitetne, jake lozinke (dobra entropija!)
  - Nametati ograničenja kompleksnosti lozinke
  - Koristiti fraze (passphrases) umjesto lozinki
- Ograničavanje broja pokušaja, zaključavanje
  - Ubacivanje kašnjenja između dva pokušaja
  - Nakon N pokušaja privremeno ili permanentno zaključavanje korisničkog računa
- Primjena jačih autentifikacijskih metoda (PKI, 2FA, …)
- Pohrana lozinki u šifriranom obliku ili u obliku sažetka
  - Zaštita od „off-line” pogađanja

Nekorištenje šifrirane komunikacije

- Mnogi protokoli šalju podatke preko mreže u čistom obliku
  - Snimanjem prometa moguće je ukrasti osjetljive podatke
  - Dosta često slanje lozinke preko mreže
- Mnogi aplikacijski protokoli su ranjivi na prisluškivanje
  - Posebno su kritični aplikacijski protokoli temeljeni na UDP-u
    - TLS se ne može koristiti, a DTLS nije toliko zaživio
- Zaštite
  - Šifriranje na nižim slojevima (IPsec, TLS)
  - Tuneliranje korištenjem aplikacije SSH ili neke slične metode
  - Korištenje autentifikacijskih protokola koji ne prenose lozinke preko mreže
  - Noviji protokoli razvijaju se s „ugrađenom” enkripcijom, npr. QUIC/HTTP3

Poslužitelji elektroničke pošte

- Elektronička pošta koristi barem dva poslužitelja
  - MTA - Mail Transfer Agent (postfix, sendmail, qmail, …)
  - MUA - Mail User Agent / MDA - Mail Delivery Agent (dovecot, …)
- Danas je uobičajeno integrirano rješenje (tzv. groupware)
  - MS Exchange, Zimbra, Lotus Notes
  - Značajno povećana kompleksnost sustava što znači i vjerojatnije pogreške
  - Mogućnost korištenja jednostavnijeg posredničkog poslužitelja radi sigurnosti
- Poslužitelj elektroničke pošte direktno izložen na Internetu
  - Sprečavanje pristupa bi onemogućilo primanje elektroničke pošte
- Obavezna redovita nadogradnja

Usluga prijenosa datoteka (1)

- Originalno za tu namjenu bio je predviđen protokol FTP
  - File Transfer Protocol
- Jedna od primjena je anonimni „upload” i „download” datoteka
  - Neispravnim podešavanjem moguće je napadačima omogućiti postavljanje nedozvoljenih sadržaja, dohvat postojećih „skvirenih” datoteka, brisanje sadržaja, čitanje i pisanje direktorija na poslužitelju kojima se ne bi smjelo pristupiti
  - Napadači su znali razmjenjivati piratizirani materijal zloupotrebom anonimnih FTP poslužitelja
- Nema zaštitu komunikacije, prijenos lozinke preko mreže
  - Postoji ekstenzija FTPS, ali se ne koristi često

Usluga prijenosa datoteka (2)

- Protokol uključuje otvaranje zasebnih TCP veza!
  - Kontrolni kanal koristi jednu TCP vezu, za svaki prijenos podataka otvara se zasebna TCP veza
  - Otvaranje zasebne veze može biti u aktivnom i pasivnom modu
    - Aktivni način -> poslužitelj se spaja na klijenta
    - Pasivni način -> klijent se spaja na poslužitelj
- Povećava kompleksnost uređaja vatrozid/NAT
- Preporuka: izbjegavati
  - Alternativa SFTP/SCP
  - Ne koristiti anonimni pristup

Udaljeni rad

- Najpoznatiji protokol: SSH
  - Zamijenio telnet, r naredbe (rsh, rlogin, rcp), ftp
  - OpenSSH – najpoznatija implementacija, otvorenog koda, Unix/Linux, Windows
  - PuTTY – poznati klijent na Windows operacijskom sustavu
  - WinSCP – za prijenos datoteka na Windows OS-ovima
- Postoje i komercijalne implementacije (SecureCRT)
  - U odnosu na OpenSSH jedina prednost je GUI sučelje

Slojevi protokola SSH

SSH User Authentication Protocol autentifikacija klijenta poslužitelju	**SSH Connection Protocol** multipleksiranje šifriranih tunela u nekoliko logičkih kanala
SSH Transport Layer Protocol autentifikacija poslužitelja, povjerljivost i integritet podataka te opcionalno komprimiranje podataka	
TCP pouzdana konekcijski orijentirana dostava s kraja na kraj	
IP (nepouzdana) dostava datagrama kroz mrežu	

SSH Transport Layer Protocol

- Dogovara način razmjene ključeva, asimetrični algoritam šifriranja, simetrični algoritam šifriranja, algoritam za autentifikaciju poruka i algoritam kriptografskog sažetka
  - klijent i poslužitelj razmijene uređene liste podržanih algoritama
  - odabire se prvi algoritam koji se nalazi na popisu klijenta, a ujedno je podržan od strane poslužitelja
  - ako se ne može pronaći zajednički algoritam, veza se prekida

SSH Transport Layer Protocol

- Autentifikacija poslužitelja korištenjem para ključeva (javni/privatni)
  - poslužitelj može imati više ključeva za različite asimetrične algoritme
  - više poslužitelja može dijeliti isti ključ
- Prilikom prvog spajanja klijentski program korisniku prikazuje sažetak poslužiteljskog ključa
  - Od korisnika se očekuje provjera ispravnosti sažetka kako bi se spriječio MITM
  - Nakon provjere korisnik bi trebao potvrditi ispravnost sažetka ključa (Leap of faith)
  - Klijentski program zapisuje ključ lokalno i više ga ne predočava korisniku, ali ga obavezno provjerava prilikom svakog spajanja `~/.ssh/known_hosts`

Podržane autentifikacije klijenta

- Prijava upotrebom korisničkog imena i lozinke
- Upotreba asimetrične kriptografije
  - Klijent generira par javni-tajni ključ
  - Tajni ključ može i treba biti zaštićen lozinkom
  - Javni ključ instalira na svako računalo kojemu želi pristupiti (`~/.ssh/authorized_keys`)
- Podržano je još
  - PKI, Kerberos, PKCS11, integracija s PAM sustavom na Linuxu, 2FA, …

Usluge temeljene na protokolu SSH

- Udaljen rad (ssh klijent)
- Prijenos datoteka (scp i sftp klijenti)
- Tuneliranje Ethernet okvira ili IP datagrama
  - Ostvarivanje VPN-ova na drugom ili trećem sloju
- Prosljeđivanje (engl. forwarding) lokalnih i udaljenih pristupa
  - Spajanjem na lokalni pristup otvara se veza na udaljenom računalu prema nekom drugom pristupu/IP adresi (prosljeđivanje lokalnog pristupa)
  - Spajanjem na pristup udaljenog računala otvara se veza na neki pristup lokalnog računala (prosljeđivanje udaljenog pristupa)

Mogući operativni problemi sa SSH

- Korisnik nije zaštitio tajni ključ lozinkom
  - Omogućava napadaču neometan pristup svim računalima na koje se može prijaviti bez lozinke
  - To je posebno kritično kada se pristupa administratorskim računima, i/ili se tajni ključ nalazi na slabije zaštićenim radnim stanicama administratora
- Popis računala i javnih ključeva
  - Omogućava napadaču enumeraciju računala bez velikog problema
  - U novijim verzijama pohranjuje se sažetak imena računala
- Zamjena i povlačenje ključeva je zahtjevna
  - Primjerice kada netko ode iz tvrtke

DNS

Svrha napada na sustav DNS

- Sprečavanje pristup određenoj usluzi
  - Primjerice, slanje negativnih odgovora (kao da DNS naziv ne postoji)
  - Preusmjeravanje zahtjeva na poslužitelj koji ne sadrži traženu uslugu ili ne postoji
- MITM napad ili podmetanje lažnih sjedišta
  - Preusmjeravanja komunikacije te potom prosljeđivanje pravom odredištu
  - Varijacija napada je prerušavanje (predstavljanje) kao pravi poslužitelj
  - Ranjivi su Web poslužitelji i poslužitelji elektroničke pošte, ali i drugi poslužitelji
- Preuzimanje domena
  - Kompromitiranjem nesigurnih mehanizama osvježavanja preuzima se domena

Prijetnje sustavu DNS (1)

- Presretanje paketa
  - Napadač izvršava MITM napad te presreće kompletnu komunikaciju
  - Praćenje upita i slanje lažiranih odgovora koji stižu prije legitimnih
  - Napadaču olakšava napad činjenica da se odgovor sastoji od samo jednog UDP paketa
  - Napadač ne mora falsificirati ili na neki drugi način utjecati na sam odgovor, može podmetati i lažne informacije u drugim dijelovima poruke
- Primjena IPsec/TLS i sličnih rješenja nije odgovarajuća
  - Štiti samo pojedine korake, ne s kraja na kraj
  - Zahtjeva uspostavu povjerenja između svih strana
  - Za opterećene poslužitelje značajno podiže opterećenje

Prijetnje sustavu DNS (2)

- Pogađanje ID vrijednosti i predviđanje upita
  - engl. ID Guessing and Query Prediction
  - Napadač nije na putu i mora pogoditi ID u paketu te izvorišni pristup
    - U određenim situacijama izvorišni pristup je fiksiran na 53
    - Broj pokušaja je 2^32, odnosno 2^16
    - Naravno da napadač mora znati QNAME i QTYPE
  - Napadač može koristiti i dodatne informacije kako bi smanjio broj pokušaja
    - Primjerice, predvidivo generiranje ID-jeva i pristupa
- Zaštita
  - Isti komentari kao i za presretanje paketa

Prijetnje sustavu DNS (3)

- „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
  - U priručni spremnik može se ubaciti informacija koja nije direktno tražena od strane žrtve, ali će ju onda žrtva koristiti
- Zaštita
  - Djelomična zaštita sprečavanja trovanja priručne memorije je provjera relevantnosti dobivenih informacija s obzirom na poslani upit
    - Napad povezivanja imena se ne može tako spriječiti!

Prijetnje sustavu DNS (4)

- Manipulacija upotrebom poslužiteljima
  - engl. Betrayal By Trusted Server
  - Klijent vjeruje nekom poslužitelju koji je pod kontrolom napadača ili se jednostavno ne ponaša u skladu s očekivanjima
  - Ne mora nužno biti autoritativni poslužitelj
- Uskraćivanje usluge
  - Oko ove prijetnje nije moguće napraviti puno dizajnom protokola (kao u slučaju TLS-a)
  - Rješava se višestrukim DNS poslužiteljima po domeni razmještenima u različitim mrežama
  - Ponekad (pogotovo u slučaju korijenskih poslužitelja) rješava se upotrebom ANYCAST adresa

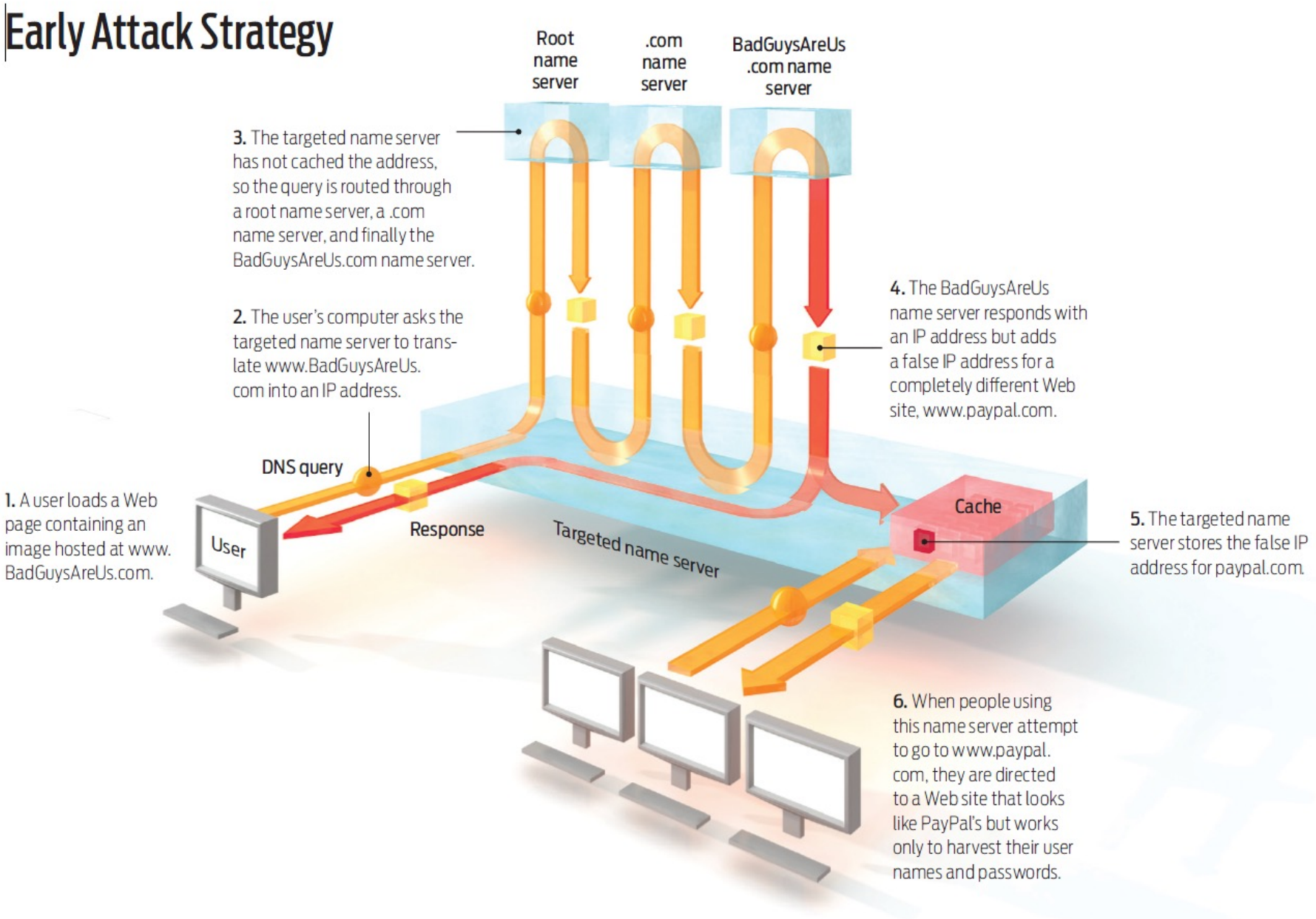
Primjer napada: „DNS Cache poisoning”

```
User Datagram Protocol, Src Port: 52046 (52046), Dst Port: domain (53)
Domain Name System (query)
    [Response In: 454]
    Transaction ID: 0x2e49
  Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    newsroom.cisco.com: type A, cl
        Name: newsroom.cisco.com
        Type: A (Host address)
        Class: IN (0x0001)
```

```
User Datagram Protocol, Src Port: domain (53), Dst Port: 52046 (52046)
Domain Name System (response)
    [Request In: 422]
    [Time: 0.136090000 seconds]
    Transaction ID: 0x2e49
  Flags: 0x8480 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  Queries
    newsroom.cisco.com: type A, class IN
        Name: newsroom.cisco.com
        Type: A (Host address)
        Class: IN (0x0001)
  Answers
    newsroom.cisco.com: type A, class IN, addr 198.133.219.119
  Authoritative nameservers
    newsroom.cisco.com: type NS, class IN, ns ns2.cisco.com
    newsroom.cisco.com: type NS, class IN, ns ns1.cisco.com
  Additional records
    ns1.cisco.com: type A, class IN, addr 128.107.241.185
    ns2.cisco.com: type A, class IN, addr 64.102.255.44
```

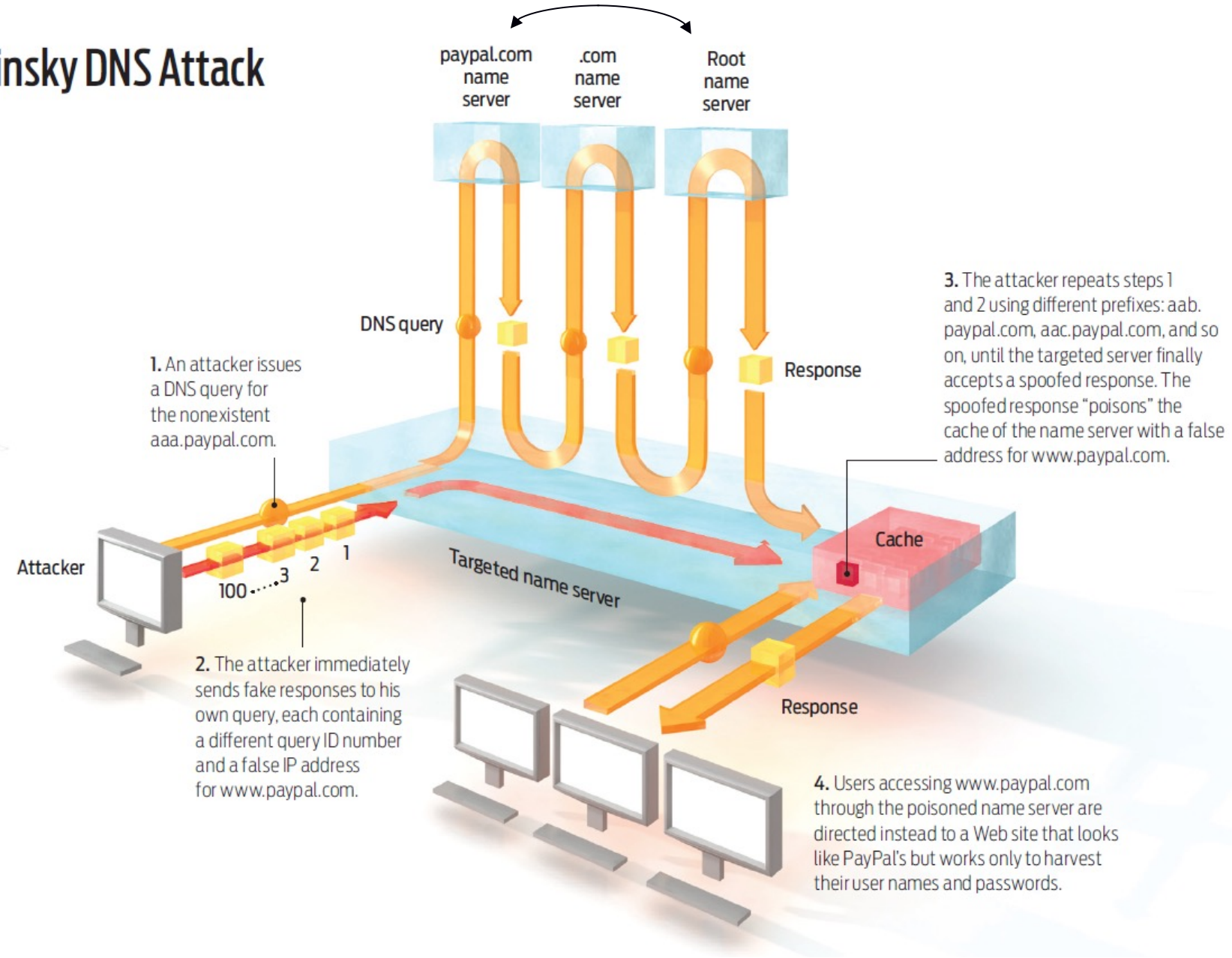
- DNS upit i odgovor:

DNS Cache poisoning



Kopirano iz:
http://spectrum.ieee.org/oct08/6818

DNS Cache poisoning



Kopirano iz:
http://spectrum.ieee.org/oct08/6818

Zaštita od DNS Cache Poisoning

- TXID (16 bita) + „random source port” (16 bita)
- Napad na DNS „forwarder” (dnsmasq): DNSpooq
  - https://www.jsof-tech.com/wp-content/uploads/2021/01/DNSpooq-Technical-WP.pdf
  - koristi se „random port” ali 1 od 64 i uz to napadač mora pogoditi jedan, bilo koji od tih 64 portova: umjesto 2^{32} kombinacija $2^{32}/64=2^{26}$
  - interno se upiti prikazuju u zapisu "forward record" i napadač treba pogoditi TXID i podatke u odgovarajućem "forward record”
  - ne pamti se cijeli forward record već samo "hash" i to prilagođena verzija CRC32 (nije kriptografski sažetak i jednostavno ga je generirati)
  - dnsmasq dozvoljava višestruke zahtjeve s istim nazivom te prihvaća ispravan odgovor na bilo koji od njih
  - potrebno je ~2^{19} upita za uspješan cache poisoning

  . . .

Zaštita sustava DNS: Mehanizam TSIG

- Definirano u svibnju 2000. godine
- Temelji se na dijeljenom ključu uz pomoć kojega se generira potpis
  - Problem raspodijele ključeva!
- Koristi se za dinamička osvježavanja zone te za prijenos zone na sekundarne poslužitelje
- Podržanim DNS zahtjevima dodaje se TSIG RR
  - Sadrži identifikator ključa koji se koristi za potpisivanje
  - Informacije o algoritmu te vremenu potpisivanja
  - Potpis

Zaštita sustava DNS: DNSSEC (1)

- engl. Domain Name System Security Extensions
- Osigurava kriptografski dokaz ispravnosti primljenih podataka
- DNSSEC ne osigurava
  - Dinamičko osvježavanje podataka na glavnom DNS poslužitelju (engl. master)
  - Prijenos podataka o zoni (master → slave)
- Klijenti korištenjem resolvera koji provjeravaju valjanost dobivaju zajamčeno sigurne podatke
  - Za podatke koje ne može provjeriti resolver vraća SERVFAIL

Zaštita sustava DNS: DNSSEC (2)

- Za zaštitu se koristi asimetrična kriptografija
- Podaci, zapisi na poslužitelju (RR – Resource Records), potpisuju se privatnim ključem
  - Javni ključ se objavljuje putem DNS-a i koristi se za provjeru valjanosti potpisa
- Potpisom se osigurava valjanost zapisa s kraja na kraj – između autoritativnog poslužitelja i resolvera
  - Valjanost podataka znači autentičnost izvora podataka i integritet
  - Autentičnost negiranja postojanja zapisa (NXDOMAIN)
- Možemo li tim podacima vjerovati?
  - Da ako je root (“.”) potpisan!

Zaštita sustava DNS: DNSSEC (3)

- Novi zapisi za podršku DNSSEC [RFC 4034]
  - Resource Record Signature (RRSIG)
  - DNS Public Key (DNSKEY)
  - Delegation Signer (DS)
  - Next Secure (NSEC)
- Nove zastavice u zaglavlju DNS paketa:
  - Checking Disabled (CD), Authenticated Data (AD)
  - Nužna podrška EDNS0 (Extension Mechanisms for DNS)
- Novi bitovi u zaglavlju (temeljeni na EDNS0):
  - DNSSEC OK (DO) – resolver je spreman primiti DNSSEC RR

Primjer

```
$ dig -t any . @a.root-servers.net
;; ANSWER SECTION:
.                       86400   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2021050600 1800
900 604800 86400
.                       86400   IN      RRSIG   SOA 8 0 86400 20210519050000 20210506040000 14631 .
PPxbJDLay5PKFc3FqA+fB6aHXnjLk0/nBZah+WF30Mgxprwx0Wq7JaXM
......
.                       518400  IN      RRSIG   NS 8 0 518400 20210519050000 20210506040000 14631 .
asV1d3Tpp5hHzod7QiDD9avSLtbbjCT0v3tV0VoKd5rIwfyhOpbtESdG bz2em4kYzmXinat8Fj3aEB3m5tPTpKXTFsWvjWLpWNRXWU3AF3pFz/N0
......
.                       86400   IN      RRSIG   NSEC 8 0 86400 20210519050000 20210506040000 14631 .
f4OAP9oB2VltEQDDftR2iCcrlMGzoBK4UmSjwyFQILj3FPTVc6ZImW97 plkR5bd3GtwEIp0eDL5EUymQet8hOaQM5BMEaC69kP7NmjntEx4ffSRw
......
.                       172800  IN      RRSIG   DNSKEY 8 0 172800 20210522000000 20210501000000 20326 .
KTOHq4gvmIC2KJOzZwQhHGonCSPCCEtX/453Ow6uauO3BjuoNp3Bdjh2 BxEaHBQ5mvp+n/WjsrlQdQvuf1BSZfVUJoOm3ofTQI6rRpex3rYxj8BY
......
.                       518400  IN      NS      a.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       172800  IN      DNSKEY  256 3 8
AwEAAa+HvD7XXjmL+1htThUQyZW7oWGnjzKHJASg3TSR5Bmu5LfnSVW7 fxqZa2oAYo2ionIQWyqAj/loApzg8GNMhyIibftPJso54uWRQ2GaoMrw
a.root-servers.net. 518400  IN      A       198.41.0.4
b.root-servers.net. 518400  IN      A       199.9.14.201
......
```

Problemi sustava DNSSEC

- DNSSEC ne osigurava povjerljivost podataka
  - To je namjerna odluka donesena na početku razvoja protokola
- DNSSEC ne štiti od DDoS napada
- Utjecaj na mrežu i vatrozide
  - Očekuju se puno duži odgovori (do 2KB)
  - Vatrozid ne smije mijenjati DNS odgovore – potpis neće odgovarati
- Vrijeme života digitalnog potpisa
- Kod svake promjene podataka zonu treba ponovo potpisati
- Ključeve treba povremeno mijenjati – više posla!

...

- Napad na DNS „forwarder” (dnsmasq): DNSpooq
  - Bug u implementaciji: ako se koristi DNSSEC, ranjivost tipa „buffer overflow” kod provjere valjanosti odgovora!

Neke druge (zlo)upotrebe DNS-a

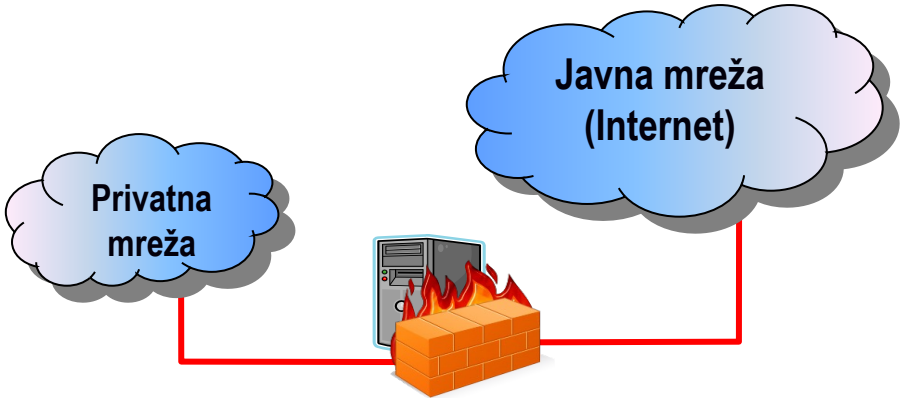
- DNS sve više služi za raspodijelu sigurnosno osjetljivih podataka
  - Distribucija javnih SSH ključeva poslužitelja
  - Osiguravanje elektroničke pošte
  - Podaci o autentifikacijskom sustavima u tvrtkama
- Autorizacija i autentifikacija na temelju imena domene
  - Napadač može lažirati upite za reverznim razrješavanjem
- Napadači zloupotrebljavaju DNS
  - Eksfiltracija podataka iz tvrtke
  - Upravljanje zaraženim računalima (botovima)
    - Zato se DNS koristi za detekciju zaraženih računala u unutarnjoj mreži (pristup „neobičnim” domenama)

“DNS over TLS” / “DNS over HTTPS”

- Problem privatnosti, skrivanje meta-podataka
- DNS over HTTPS
  - RFC 8484: "DNS Queries over HTTPS (DoH)”
  - HTTPS i HTTP/2, port 443 (DNS promet "skriven" unutar ostalog šifriranog prometa)
- DNS over TLS
  - RFC 7858: "Specification for DNS over Transport Layer Security”
  - RFC 8310: "Usage Profiles for DNS over TLS and DNS over DTLS”
  - TCP + TLS, port 853
- Cloudflare DNS resolver: 1.1.1.1 i 1.0.0.1 podržava oba standarda
  - https://blog.cloudflare.com/dns-resolver-1-1-1-1/

Vatrozid

Vatrozid (1)



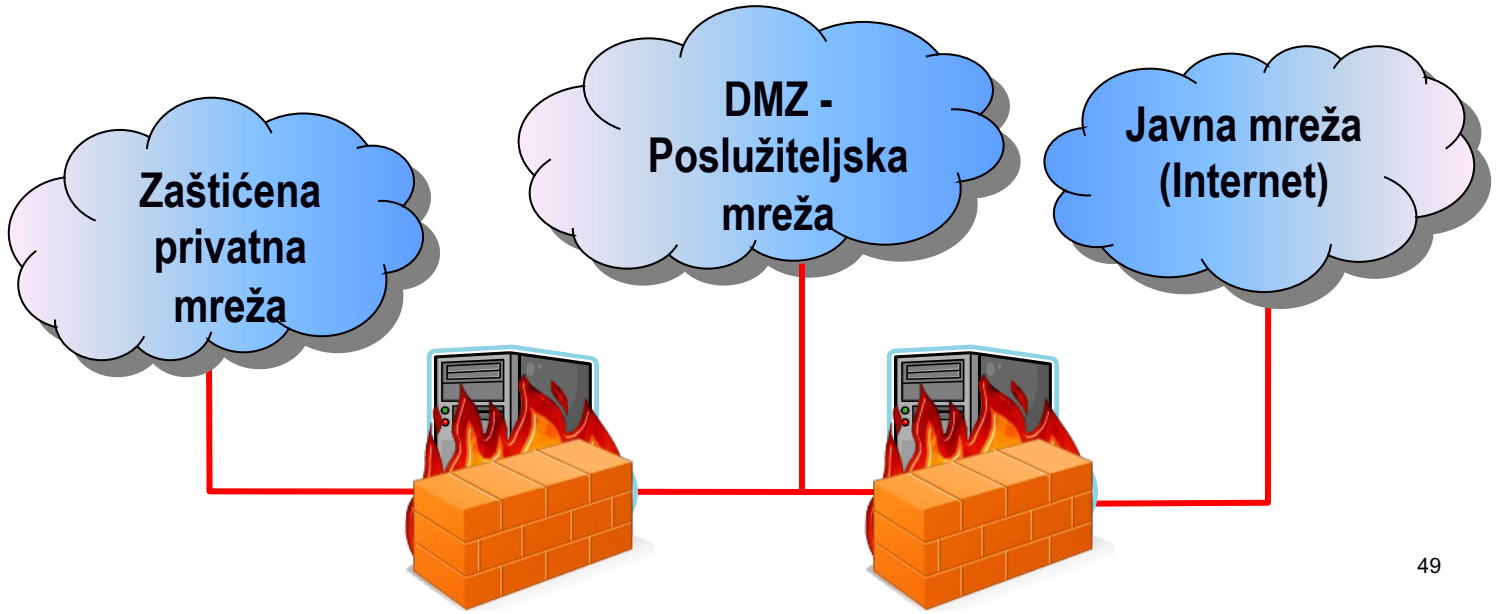
- Firewall – vatrozid, sigurnosna stijena
- Uređaj koji radi na mrežnom sloju
- Smješten između dvije ili više mreža
  - Mreže su različite razine povjerenja (nekima vjerujemo manje drugima više)
  - Najčešće između dvije mreže od kojih je jedna Internet (Internet je mreža najniže razine povjerenja)
- Princip rada vrlo jednostavan
  - Provodi sigurnosnu politiku kontrolom pristupa
  - Svaki paket koji prolazi provjerava se sa bazom pravila koja određuje što treba učiniti s paketom (temeljne odluke su propustiti ili odbaciti)

Arhitekture mreža s vatrozidom

- Omogućen je pristup Internetu iz privatne mreže.
- Pristup privatnoj mreži iz Interneta je zabranjen.
- Vanjske usluge, kao što su web poslužitelj, DNS poslužitelj, FTP poslužitelj, poslužitelj e-pošte smještene su u zasebnu mrežu, DMZ
  - Demilitarizirana zona

Arhitekture mreža s vatrozidom

- Privatna mreža može biti zaštićena dodatnim vatrozidom koji filtrira promet između DMZ-a i LAN-a



Packet filter

- Osnovni princip rada vatrozida je filtriranje paketa između unutarnjih i vanjskih sučelja
- Propušta ili blokira određene tipove paketa na temelju:
  - protokola (TCP, UDP, ICMP, ...), IP adresa izvora / odredišta, TCP ili UDP izvorišni / odredišni *port,* TCP zastavica (SYN, ACK, FIN, …), tipa ICMP poruke, …
- prednosti
  - jednostavna implementacija (postojeći hardver) i dobre performanse
- ograničenja
  - ograničena provjera, složena konfiguracija, nije dovoljno fleksibilno i proširivo, može biti ranjivo na *spoofing*, problemi s fragmentiranim datagramima

Statefull Inspection

- radi kao paket filter (pristupne liste) + održavanje stanja
  - provjera i održavanje informacije o stanju svake konekcije
- dohvaća i informacije iz protokola na višim slojevima
  - moguće je pratiti slijed sesije (na primjer za FTP)
  - virtualne sesije za beskonekcijske protokole (UDP)
    - vatrozid sprema podatke o *portovima* korištenim u određenim UDP transakcijama
    - kreiraju se privremena pravila koja propuštaju odgovor
  - provjera svakog paketa
    - ponekad se preskače provjera paketa koji je dio uspostavljene konekcije

Primjer vatrozida: netfilter / iptables (Linux)

- `iptables` se koristi za postavljanje, održavanje i provjeru pravila IP vatrozida ugrađenog u Linux kernel (netfilter)
  - https://netfilter.org/documentation/index.html#documentation-howto
- Pravila su organizirana u tablice (lance, "*chains*")
  - Mogu se pridružiti različitim fazama obrade datagrama
  - Pravila se obrađuju slijedno
  - stuffphilwrites.com/wp-content/uploads/2018/09/FW-IDS-iptables-Flowchart-2018-09-01.png
- Ugrađene tablice:
  - INPUT – za pakete kojima je odredište na vatrozidu
  - FORWARD – za pakete koji se prosljeđuju (usmjeravaju) kroz vatrozid (odredište nije na vatrozidu)
  - OUTPUT – za pakete koji su lokalno generirani (na vatrozidu)

iptables

- Pravila se obrađuju slijedno
- Ako paket zadovoljava zadani uzorak izvodi se definirana akcija, skok („jump”) na sljedeći lanac
- 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)

  Primjer:

```
# iptables  -A FORWARD  -p TCP  -d 161.53.72.120  --
   dport 80  -j ACCEPT
```

Naredbe

-A, --append dodaj pravilo na kraj

```
iptables –A INPUT ––dport 22 –j ACCEPT
```

-D, --delete obriši pravilo

```
iptables –D INPUT ––dport 80 –j DROP
```

-I, --insert ubaci pravilo pod definiranim rednim brojem

```
iptables –I  INPUT 1 ––dport 80 –j ACCEPT
```

-L, --list ispiši pravila

```
iptables –L INPUT –n –v
```

-F, --flush obriši sva pravila definiranog lanca

```
iptables –F INPUT
```

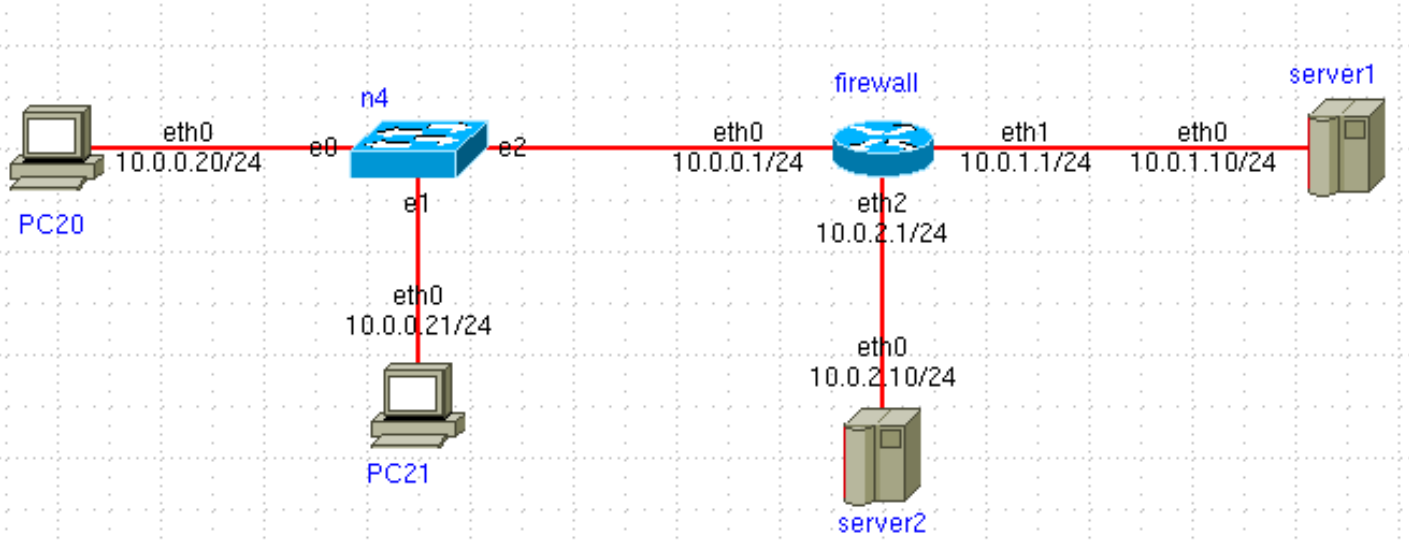
-P, -- policy *defaultna* politika (implicitno zadnje pravilo)

```
iptables –P INPUT DROP
```

Uzorci u filterima

- generički uzorci
  - **-p** --protocol na primjer tcp, udp, icmp
  - **-s** --src izvorišna IP adresa
  - **-d** --dst odredišna IP adresa, na primjer 10.1.2.3 ili 10.2.3.0/24
  - **-i** --in-interface dolazno sučelje, na primjer eth0
  - **-o** --out-interface odlazno sučelje
- uzorci za protokole UDP i TCP (-p udp ili -p tcp)
  - **--sport** --source-port izvorišni port
  - **--dport** --destination-port odredišni port
- uzorci za protokol ICMP (-p icmp)
  - **--icmp-type** tip icmp poruke, na primjer „echo request”: --icmp-type 8
- stanje konekcije:
  - **-m state ESTABLISHED, RELATED**
  - -m conntrack --ctstate ESTABLISHED, RELATED

Primjeri korištenja




```
firewall#   iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)

firewall#   iptables -P INPUT DROP
firewall#   iptables -P OUTPUT DROP
firewall#   iptables -P FORWARD DROP
```

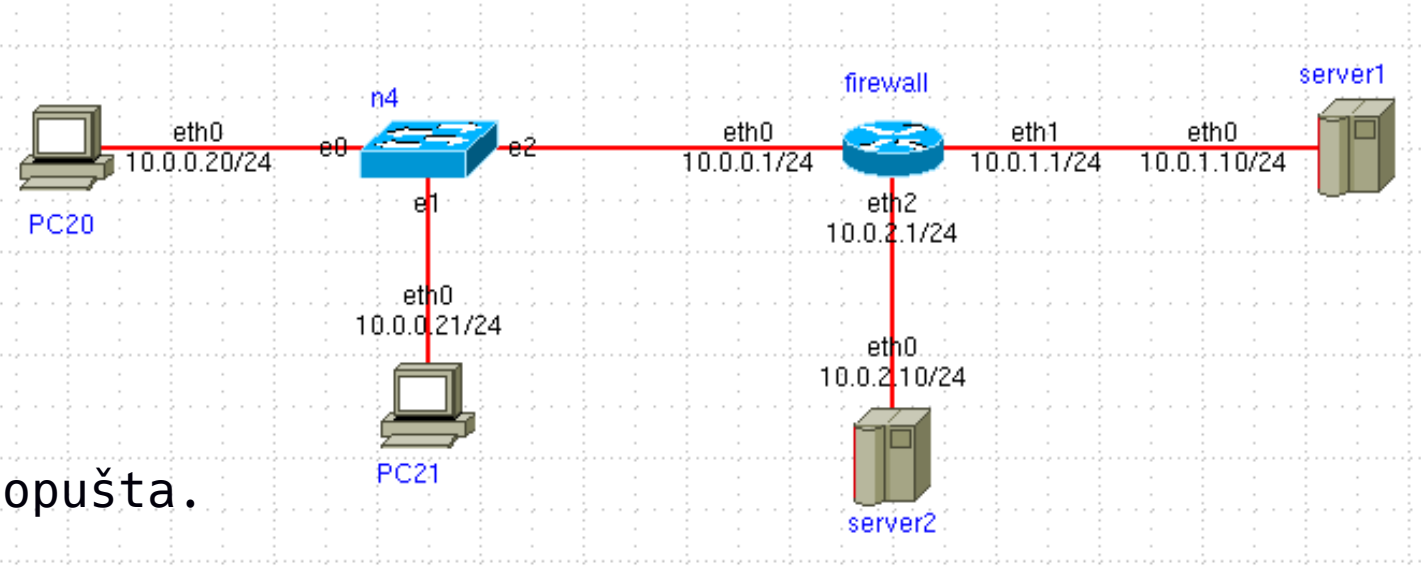
Double-click na “firewall” ili iz terminala pozvati:

```
$ sudo himage firewall iptables -L -v
```

or

```
$ sudo himage firewall
firewall#
```

Primjeri korištenja



PC20# ssh 10.0.1.10

→ne prolazi, na eth0@firewall
dolazi SYN ali ga firewall ne propušta.

 # iptables -A FORWARD -p tcp -s 10.0.0.20 -d 10.0.1.10 --dport 22 -j ACCEPT

PC20# ssh 10.0.1.10

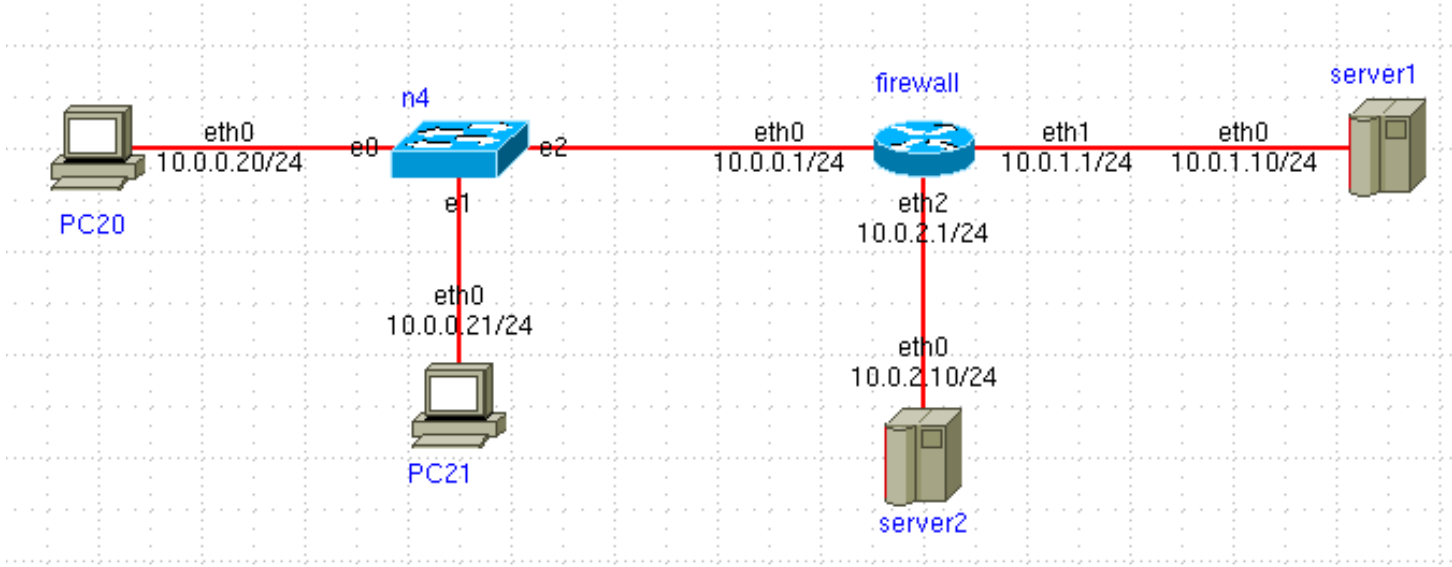
→ i dalje ne prolazi, na server1 dolazi SYN, on vraća SYN+ACK ali firewall to ne propušta (paket se vidi na eth1@firewall)

 # iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

PC20# ssh 10.0.1.10 ← prolazi jer je “established”

The authenticity of host '10.0.1.10 (10.0.1.10)' can't be established.

Primjeri korištenja




```
# iptables -A FORWARD -p icmp \
      -s 10.0.1.10 -j ACCEPT
```

```
# himage server1 ping 10.0.0.20
64 bytes from 10.0.0.20: icmp_seq=34 ttl=63 time=0.269 ms
→Prolazi i odgovor jer je “established”!

# himage PC20 ping 10.0.1.10
→ ne prolazi jer nije “established”!
# himage server2 nc -u -l -p 1234
```

```
# iptables -A FORWARD -p udp -d 10.0.2.10 --dport 1234 -j ACCEPT
```

```
# himage PC20 nc  -u  10.0.2.10 1234
→ prolazi (“established”!)
```

Završne napomene o vatrozidu

- Vatrozid je uređaj mrežnog sloja. No, s obzirom da su mu mogućnosti u tom slučaju ograničene svoju funkcionalnost obavlja i na prijenosnom sloju.
- Prilikom kupovine često je sva funkcionalnost upakirana u jedan uređaj koji proizvođači nazivaju samo vatrozid
- Vatrozid nije rješenje svih problema sigurnosti(!)
  - Sve više aplikacija koristi HTTP za komunikaciju kako bi zaobišli vatrozide.
- Jednostavni uređaji ali u primjeni vrlo kompleksni
  - Mreža vatrozida
  - Mnoštvo pravila

Posrednički poslužitelji

- Vatrozid radi na 3. sloju ISO/OSI RM-a (i 4. sloju)
  - Problematično za protokole koji vrše nekakva multipleksiranja
    - Primjer protokola HTTP, virtualnih poslužitelja i URL-ova
- Posrednički poslužitelji omogućavaju bolji nadzor mrežnog prometa
  - Moguća detekcija zloćudnog koda
  - Crne i bijele liste
  - Bilježenje pristupa radi retroaktivne analize
  - Dodatno, mreža je efikasnija
- ALI: Bez vatrozida nije moguće dosljedno provoditi politiku korištenja posredničkog poslužitelja

IDS

Sustavi za detekciju upada (1)

- engl. 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

Sustavi za detekciju upada (2)

- Mrežni sustavi
  - Postavljaju se na neke ključne točke na kojima snimaju promet
    - Bitno je da vide promet mrežnog segmenta kojeg želimo pratiti
  - Mogući problemi s brzinama (10G+)
  - Problem je i šifrirana komunikacija
- Mnoštvo različitih sustava na tržištu
  - Popularna implementacija otvorenog koda - SNORT, BRO, OSSEC, Suricata

Sustavi za prevenciju upada

- Osim detekcije rade i prevenciju
  - Intrusion Prevention Systems (IPS)
- Prevencija može biti postavljanje dodatnih pravila na vatrozidu
  - Pravila privremena ili stalna
- Ako nisu dobro podešeni mogu onemogućiti ispravan rad mreže!

Otkrivanje ranjivosti u mreži

- Ranjivosti u računalnoj mreži su neizbježne(!)
  - Treba ih što prije otkriti i ukloniti
- Otkrivanje ranjivosti može se obaviti na dva temelja načina
  - Skeniranje mrežnih raspona
    - Nessus, OpenVAS
    - Jednostavno, ali opterećuje mrežu i puno lažno točnih detekcija
    - Jeftina, ali ne otkrivaju nužno sve ranjivosti
  - Penetracijska ispitivanja
    - Obavljaju pojedinci ili timovi koji traže ranjivosti
    - Cilj je i pokušati iskoristiti ranjivost, ne samo ju naći
    - Skuplja od skeniranja
    - Ne otkrivaju nužno sve ranjivosti