



Sigurnost u računarskim mrežama

IDS sistemi: prvi deo (Osnovni pojmovi i statističke karakteristike)

Nemanja Maček

- Sistemi za detekciju upada
- Komponente i arhitekture IDS sistema
- Statističke karakteristike sistema i mere performansi
- Primer: snort
- Neke tehnike zaobilaženja IDS sistema

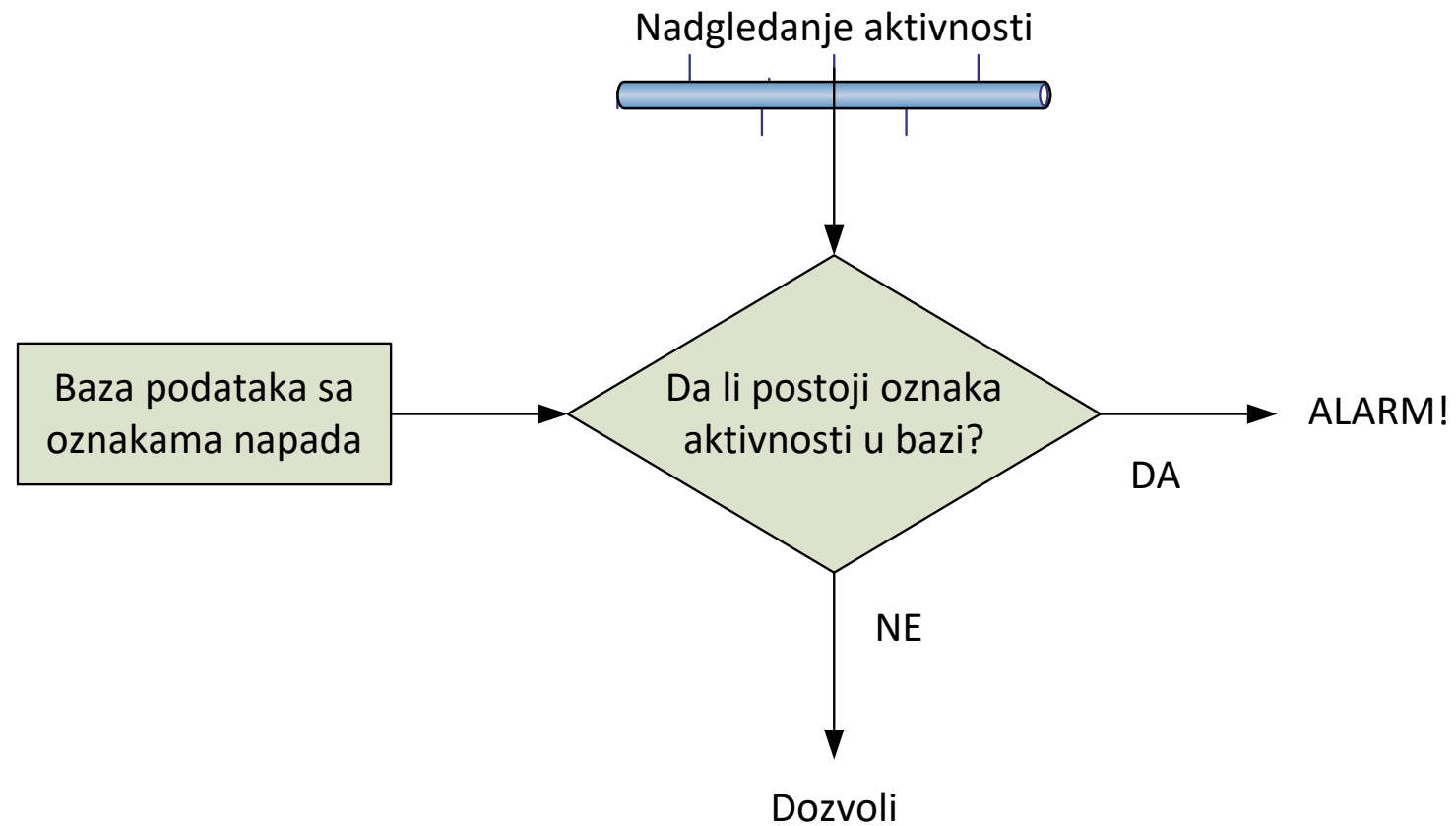
Šta su sistemi za detekciju upada?

- Džim Anderson: **upad** u računarski sistem ili mrežu je svaki neovlašćeni pokušaj
 - pristupa, izmene ili uništavanja informacija, ili
 - dovođenja sistema u nepouzđano ili neupotrebljivo stanje.
- Drugim rečima, upad je bilo koji skup akcija koji narušava **integritet**, **poverljivost** ili **raspoloživost** resursa.
- **Sistem za detekciju upada** (engl. *Intrusion Detection System*, IDS) nadgleda događaje u računarskom sistemu ili mreži i otkriva aktivnosti koje ukazuju na upade.
- Sistemi za detekciju upada su nastali kao odgovor na napade koji se ne mogu otkriti ili sprečiti drugim zaštitnim mehanizmima.
- Primer:
 - Firewall analizira samo zaglavlje IP paketa i na osnovu pravila filtriranja dozvoljava prolaz paketa kroz odredišni mrežni interfejs ili odbacuje paket.
 - Firewall ne analizira sadržaj paketa i ne može da spreči napade tipa prekoračenja bafera ili umetanja SQL koda koji su smešteni u sadržaju paketa.

- Osnovne komponente IDS sistema su: senzori, komponenta za analizu (engl. *analyzer*) i komponenta koja generiše odgovor (engl. *response*).
- **Senzori.**
- Senzori prikupljaju podatke, odnosno događaje iz okruženja.
- Postoje dve vrste senzora: senzori smešteni na računaru i mrežni senzori.
 - Shodno ovoj podeli razlikujemo termine **HIDS** (engl. *Host-based IDS*) i **NIDS** (engl. *Network IDS*).
- **Senzor smešten na računaru** prikuplja podatke sa izvora koji su interni u odnosu na računar, najčešće na nivou operativnog sistema.
 - Primer: podaci o rasporedu ili učestalosti izvršavanja sistemskih poziva.
- **Mrežni senzori** prikupljaju saobraćaj sa računarske mreže.
 - Smešteni su u mrežne adaptere, rutere, pristupne tačke ili realizovani kao zasebni uređaji.
 - Zavisno od mreže koristi se jedan ili više senzora.
 - Senzor treba da bude transparentan za ostatak mreže i da je značajno ne opterećuje.

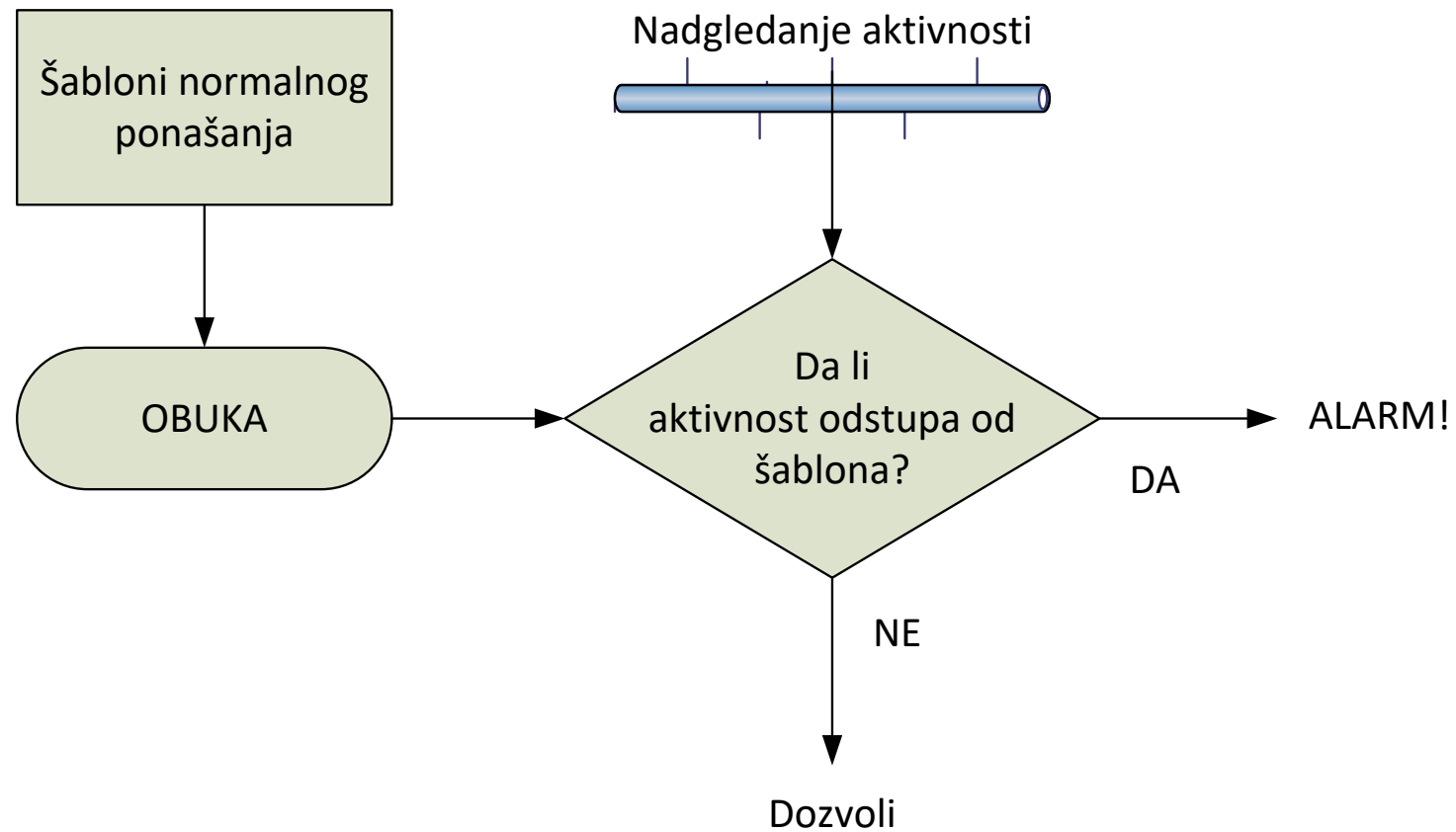
- Komponenta za analizu traži oznake **napada ili prekršaja sigurnosne polise** u podacima preuzetim sa senzora.
- Postoje dva pristupa detekciji upada: detekcija potpisa i detekcija anomalije.
- **Detekcija potpisa** je pristup zasnovan na poređenju tekuće aktivnosti sa pravilima kojima su opisani poznati napadi.
- Problem detekcije potpisa: učestalost **lažno negativnih** alarma (engl. *False Negative Rate*) može biti velika.
 - Sistem ne može otkriti nove tipove napada (napade koji nisu opisani ni jednim pravilom).
 - Sistem ne može otkriti napade koji evolviraju sa vremenom.
 - Sistem ovakve napade prijavljuje kao legitimnu aktivnost.

- **Detekcija potpisa.**



- **Detekcija anomalije** je pristup zasnovan na tehnikama pronalaženja neuobičajenih aktivnosti koje nagoveštavaju upad.
 - Primer: aktivnost korisnika koja se značajno razlikuje od prethodno definisanog šablona legitimnih aktivnosti tog korisnika.
- Problem detekcije anomalija: veliki broj **lažno pozitivnih** alarma (engl. *False Positive Rate*).
 - Sistem može legitimnu aktivnost korisnika koja se razlikuje od uobičajenog šablona ponašanja oceniti kao napad.
 - Nemoguće je predvideti sve varijacije legitimnog ponašanja!
 - Nemoguće je formirati sistem za detekciju anomalija koji ne generiše lažno pozitivne alarme!
 - Rešenje koje **smanjuje greške**: redovno ažuriranje sistema šablonima legitimnog ponašanja.
 - Jedno od rešenja problema primenljivo u HIDS sistemima:
 - Modeliranje ponašanja pojedinačnih korisnika u određenom sistemu umesto modeliranja ponašanja celokupnog sistema, tj. svih korisnika.

- **Detekcija anomalija.**



- **Hibridni pristup detekciji.**
- Detekcija potpisa je veoma efikasna za napade čije su oznake poznate IDS sistemu.
- Međutim, nemoguće je predvideti sve varijacije poznatih napada.
 - To znači da je neka vrsta detekcije anomalije neophodna.
- Hibridni IDS sistemi kombinuju oba pristupa detekcije.
- Zasnovani su na principima biološkog imunog sistema (engl. *Human Immune System*).
- IDS najpre poredi tekuću aktivnost sa oznakama poznatih napada.
 - Ukoliko je napad detektovan IDS se oglašava alarmom.
 - Ukoliko napad nije detektovan IDS poredi aktivnost sa šablonima normalnog ponašanja.
 - Ukoliko je anomalija detektovana, sistem formira oznaku.
 - Takvo ponašanje nadalje se detektuje na osnovu potpisa.

- **Komponenta koja generiše odgovor** oglašava se alarmom u slučaju da je upad detektovan.
- Komponenta može biti:
 - **Pasivna.**
 - Sistem dodaje zapis u dnevničku datoteku i eventualno obaveštava administratora sistema slanjem elektronske pošte.
 - **Aktivna.**
 - Sistem reaguje na napad.
 - Primer (NIDS): blokira određenu IP adresu ili prekida TCP konekciju.
 - Primer (HIDS): prekida proces ili sesiju koju je korisnik započeo.
- Napomena: sistem može proaktivno da reaguje na napad jedino ako komponenta za analizu detektuje upade **u toku njihovog izvršavanja!**
 - Primer: linijski (engl. *in-line*) mrežni IDS sistem).
- Sistemi koji detektuju zapisane događaje ne mogu da spreče napad!
 - U nekim slučajevima napadač može da izmeni zapisane događaje i ukloni tragove o napadu.

- Sistemi koji proaktivno reaguju na napade nazivaju se **sistemima za sprečavanje upada** (engl. *Intrusion Prevention System*, IPS) i najčešće se realizuju integrisanjem postojećih tehnologija u jedan celovit sistem.
- Primer: mrežni IPS kombinuje funkcionalnost mrežnih IDS sistema, mrežnih barijera, i dodatnih mehanizama za sprečavanje zlonamernih aktivnosti.
 - Najčešće se realizuje kao uređaj sa dva mrežna adaptera od kojih je jedan vezan sa unutrašnjom a drugi sa spoljašnjom mrežom.
- Za razliku od firewalla mrežni IPS obavlja **dubinsku analizu paketa** (engl. *deep packet inspection*).
- Faze odgovora na detektovani napad prema Met Bišopu su:
 - **Ograđivanje** (napadaču se ograničava pristup sistemskim resursima)
 - **Iskorenjivanje** (zaustavljanje napada i sprečavanje mogućnosti da se napad ponovi)
 - **Oporavak** (vraćanje sistema u stabilno stanje).

- IDS sistemi se mogu podeliti na sisteme sa jednoslojnom i višeslojnom arhitekturom.
- **Sistemi sa jednoslojnom arhitekturom.**
 - Čine ih komponente koje nezavisno prikupljaju i obrađuju podatke.
 - Nedostatak ove arhitekture: nezavisnost umanjuje sofisticiranost detekcije.
- **Sistemi sa višeslojnom arhitekturom.**
 - Komponente međusobno prosleđuju podatke jedna drugoj.
 - Izlazni podaci jedne komponente se prosleđuju drugoj komponenti kao ulazni podaci.
 - Komponenta za analizu višeslojnog IDS sistema sadrži nekoliko **agenata**.
 - Agenti najčešće obavljaju samo jednu funkciju.
 - Primer: ispitivanje konkretnog protokola u mrežnom saobraćaju.
 - Višeslojna IDS arhitektura obezbeđuje:
 - Veću efikasnost i sofisticiranost analize.
 - Kompletniju sliku opšte sigurnosne situacije na računarskoj mreži.

Statističke karakteristike i mere performansi

- Mere performansi IDS-a definišu se na osnovu broja pravih (**TP**), lažnih (**FP**) i propuštenih alarma (**FN**) i broja ispravno detektovanih dozvoljenih aktivnosti (**TN**).

Da li je IDS detektovao upad ?		DA	TP	FP
		NE	FN	TN
			DA	NE
			Da li je do upada zaista došlo ?	

Statističke karakteristike i mere performansi

- **Osetljivost** (engl. *sensitivity*) se definiše kao kao količnik broja pravih i zbira pravih i propuštenih alarma (*True Positive Rate*, TPR).

$$TPR = \frac{TP}{TP + FN} = 1 - FNR$$

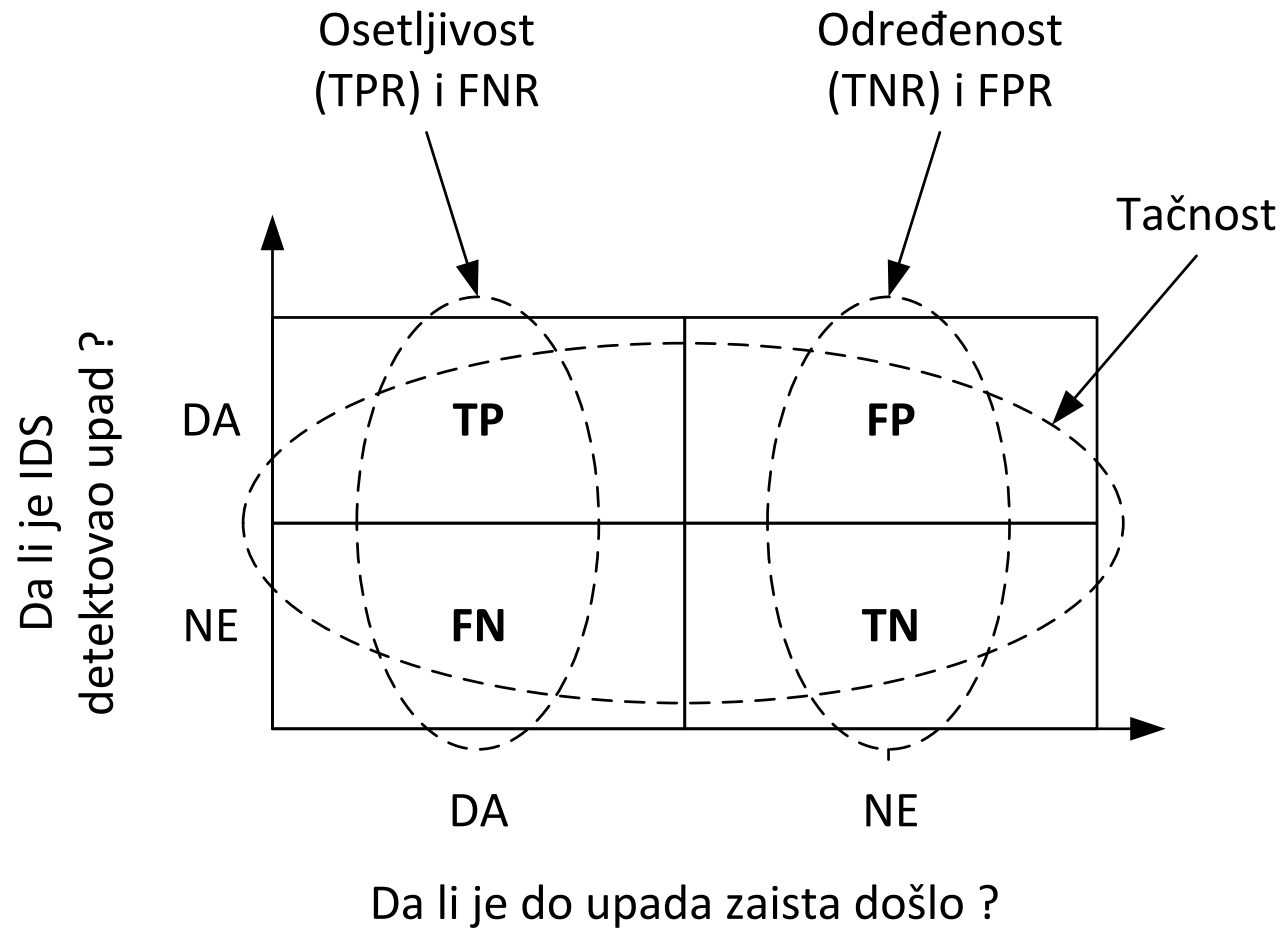
- **Određenost** (engl. *specificity*) se definiše kao kao količnik broja stvarno negativnih i zbira stvarno negativnih i lažno pozitivnih alarma (*True Negative Rate*, TNR).

$$TNR = \frac{TN}{TN + FP} = 1 - FPR$$

- U praksi se ponekad pravi kompromis između osetljivosti i određenosti.
- Najčešće se od sistema zahteva mali broj FP i FN odnosno visoka **tačnost** klasifikacije:

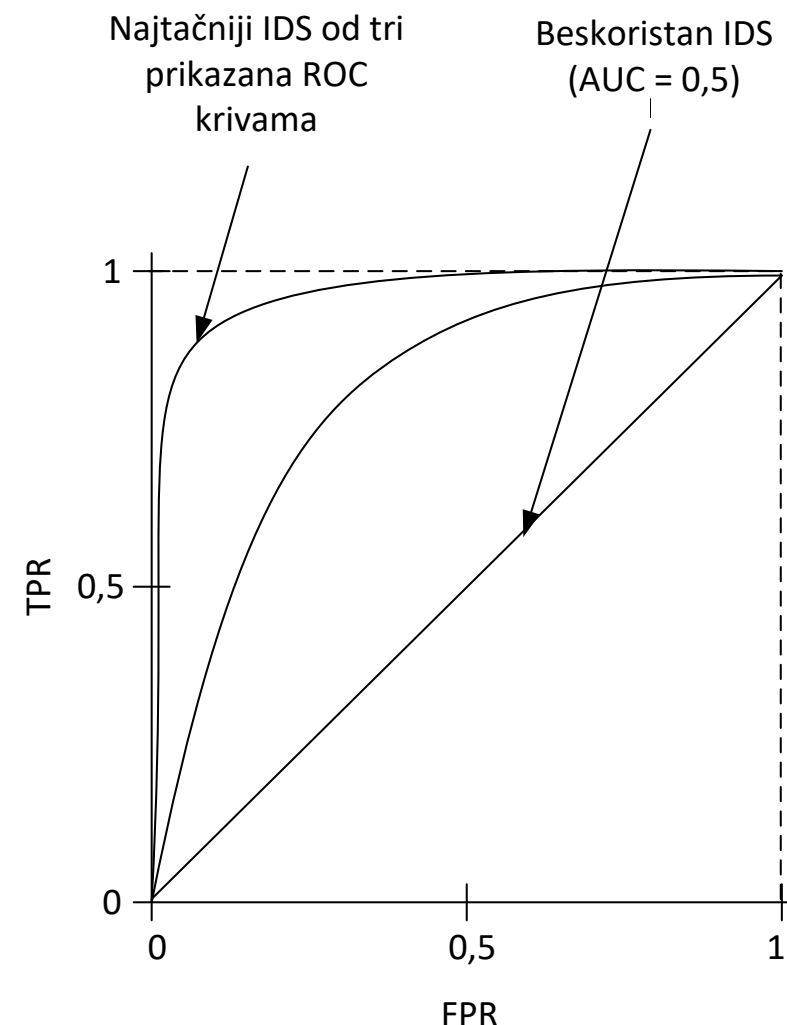
$$a = \frac{TP + TN}{TP + FP + FN}$$

Statističke karakteristike i mere performansi

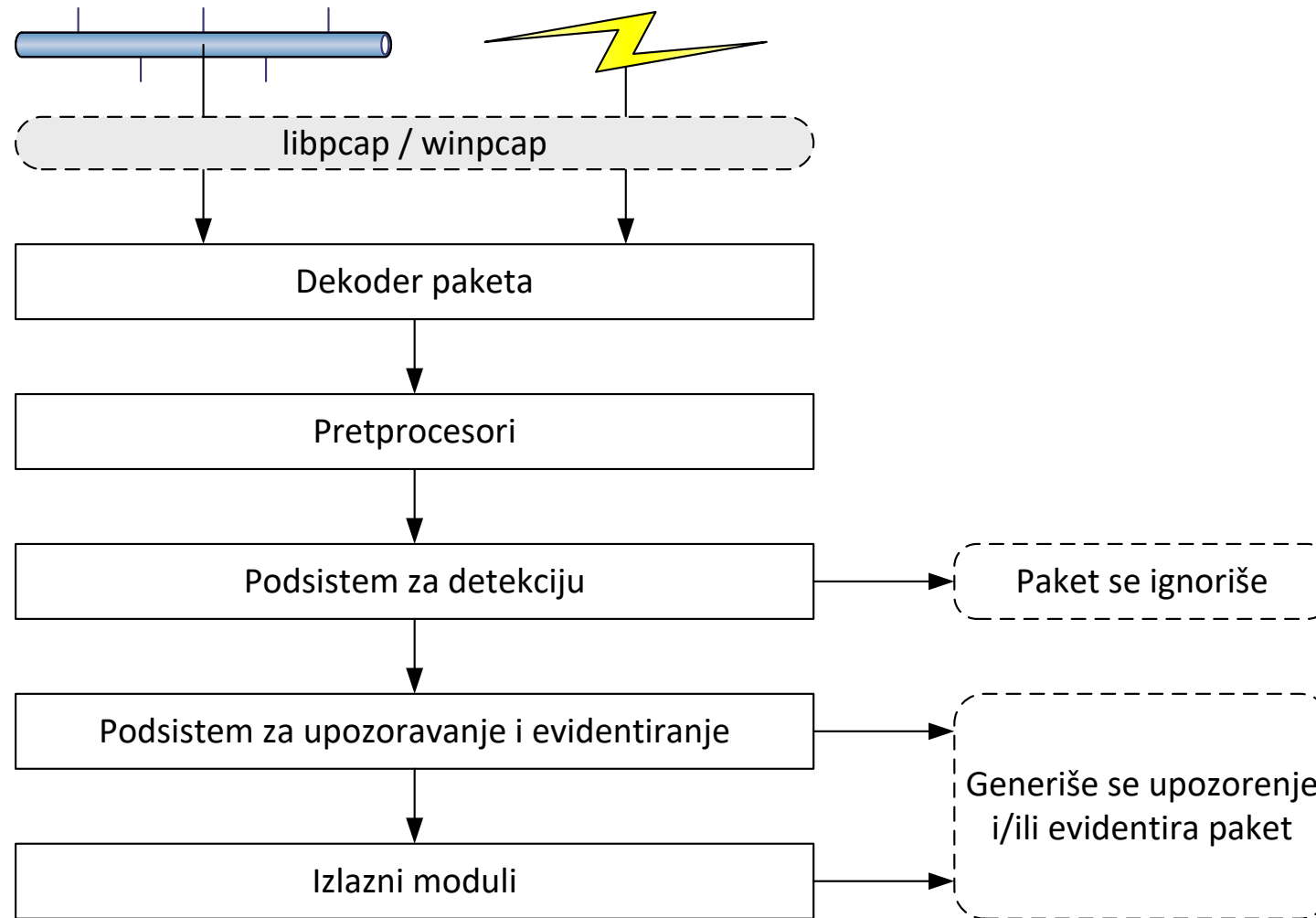


Statističke karakteristike i mere performansi

- Veza između osetljivosti i određenosti može se grafički predstaviti pomoću takozvane **ROC krive** (engl. *Receiver Operating Curve*).
- Oblik krive zavisi od celokupnog kvaliteta IDS sistema.
- Tačnost sistema određena je površiom ispod ROC krive (**AUC**, engl. *Area Under Curve*).
 - Sistem čija je kriva priljubljena uz gornji levi ugao dijagrama ima najbolje karakteristike, odnosno najveću tačnost detekcije.
 - Ukoliko je površina ispod krive 1, tačnost sistema je 100%.
 - Sistem opisan pravom linijom pod uglom od 45 stepeni (povšina ispod krive je 0,5) je beskoristan.



- Snort je Linux / Windows open-source NIDS.
- Snort analizira saobraćaj, generiše dnevničke datoteke i detektuje upade u realnom vremenu.
- Detekcija upada:
 - Na osnovu potpisa poznatih napada zadatih u vidu pravila.
 - Pomoću dodataka drugih proizvođača koji detektuju anomalije u paketima.
- Komponente Snort IDS-a:
 - libpcap / winpcap biblioteka za preuzimanje paketa sa mrežnih adaptera.
 - **Dekoder paketa** (skup komponenti koje dekodiraju protokole određenog sloja i popunjavaju strukture podataka sa dekodiranim podacima).
 - **Predprocesori** (preuređuju sadržaj paketa tako da sistem za detekciju može da otkrije upad ukoliko napadač pokušava da zavara IDS tako što će modifikovati paket).
 - **Podsistem za detekciju** (upoređuje sve pakete sa zadatim skupom pravila).
 - **Podsistem za evidentiranje i upozoravanje**.
 - **Izlazni moduli** (na primer, mogu da izmene konfiguraciju rutera ili firewall-a).



- **Režim „njuškanja“** (engl. *sniffer*).
 - Snort prati saobraćaj na mreži i prikazuje informacije o paketima na ekranu.
- **Režim evidentiranja paketa** (engl. *logger*).
 - Snort prati saobraćaj na mreži i upisuje podatke u dnevničku datoteku.
 - Podaci se mogu upisati u tekstualnu ili binarnu datoteku (tcpdump format).
- **NIDS režim.**
 - Snort ne evidentira svaki paket u dnevničkoj datoteci.
 - Ako paket odgovara nekom pravilu Snort evidentira paket ili generiše upozorenje.
 - Paket koji ne odgovara nijednom pravilu se ignoriše.
 - Dva režima:
 - Režim kratkih upozorenja (engl. *fast mode*): vreme, poruka upozorenja, izv. i odr. IP adresa i port.
 - Režim potpunih upozorenja (engl. *full mode*): dekodiraju se sva zaglavlja.
 - Za pokretanje alata Snort u NIDS režimu potrebna je konfiguraciona datoteka.

Primer Snort dnevničke datoteke otvorene u Wireshark-u

snort.log.1408367877 [Wireshark 1.10.8 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
17	4.825570	192.168.0.101	173.194.39.86	TCP	66	60027 > https [ACK] Seq=1 Ack=1 Win=29312 Len=0
18	4.825842	192.168.0.101	173.194.39.86	TLSv1.2	583	Client Hello
19	4.831083	173.194.39.85	192.168.0.101	TCP	74	https > 39294 [SYN, ACK] Seq=0 Ack=1 Win=42540
20	4.831133	192.168.0.101	173.194.39.85	TCP	66	39294 > https [ACK] Seq=1 Ack=1 Win=29312 Len=0
21	4.831341	192.168.0.101	173.194.39.85	TLSv1.2	583	Client Hello
22	4.865563	173.194.39.86	192.168.0.101	TCP	66	https > 60027 [ACK] Seq=1 Ack=518 Win=42880 Len=0
23	4.865626	173.194.39.86	192.168.0.101	TLSv1.2	247	Server Hello, Change Cipher Spec, Hello Request
24	4.865643	192.168.0.101	173.194.39.86	TCP	66	60027 > https [ACK] Seq=518 Ack=182 Win=30336 Len=0
25	4.866038	192.168.0.101	173.194.39.86	TLSv1.2	153	Change Cipher Spec, Hello Request, Hello Request
26	4.866335	192.168.0.101	173.194.39.86	TLSv1.2	131	Application Data
27	4.871028	173.194.39.85	192.168.0.101	TCP	66	https > 39294 [ACK] Seq=1 Ack=518 Win=42880 Len=0

> Frame 23: 247 bytes on wire (1976 bits), 247 bytes captured (1976 bits)

> Ethernet II, Src: Tp-LinkT_60:af:b6 (90:f6:52:60:af:b6), Dst: HonHaiPr_7f:2f:a3 (64:27:37:7f:2f:a3)

> Internet Protocol Version 4, Src: 173.194.39.86 (173.194.39.86), Dst: 192.168.0.101 (192.168.0.101)

> Transmission Control Protocol, Src Port: https (443), Dst Port: 60027 (60027), Seq: 1, Ack: 518, Len: 181

> Secure Sockets Layer

0000 64 27 37 7f 2f a3 90 f6 52 60 af b6 08 00 45 00 d'7./... R'....E.
0010 00 e9 ad 52 00 00 37 06 3f 97 ad c2 27 56 c0 a8 ...R...7. ?...'V..
0020 00 65 01 bb ea 7b 55 52 c4 37 cd 21 6a fa 80 18 .e...{UR .7.!j...
0030 02 9e ff c0 00 00 01 01 08 0a 1c c9 ea 24 00 1e\$..
0040 1b c6 16 03 03 00 7d 02 00 00 79 03 03 53 f1 fd}. ..y..S..
0050 1a 75 7e 72 07 8f 4f 1c 4e 88 a8 50 b0 1f 5a b2 .u.r..O. H..P..Z..
0060 c0 24 ab ea db e4 48 4d 13 04 f2 b5 57 20 42 44 .\$....HMW BD
0070 a4 12 d5 68 ba ef e6 62 ea 48 45 ec 5c 8a bf 2e ...h...b .HE.\...
0080 2d 23 2d ac 84 09 9b c1 d9 4a db fb 0d fe c0 2f -#.....J...../
0090 00 00 31 ff 01 00 01 00 33 74 00 28 08 73 70 64 ..1.....3t.(.spd
00a0 79 2f 35 61 31 05 68 32 2d 31 33 08 73 70 64 79 y/5a1.h2 -13.spdy
00b0 2f 33 2e 31 06 73 70 64 79 2f 33 08 68 74 74 70 /3.1.spd y/3.http
00c0 2f 31 2e 31 14 03 03 00 01 01 16 03 03 00 28 00 /1.1.... ..(.
00d0 00 00 00 00 00 00 00 3b 22 01 ce 8d 2f 80 22 ea; "....".

File: "/root/snort_logs/snort.log.1408367877" Packets: 802 · Displayed: 802 (100.0%) · Load: 0.00 · Profile: Default

- Sva Snort pravila imaju dva dela: zaglavlje i opciju.
 - **Zaglavlje** sadrži osnovni kriterijum za poređenje paketa sa pravilom (protokol, izvorišna i odredišna IP adresa i port) i akciju koja će se preduzeti ako paket zadovolji sve uslove.
 - **Deo sa opcijama** obično sadrži poruku upozorenja i dodatne informacije koje se koriste za analizu paketa, tj. za upoređivanje paketa sa pravilom.
- Snort pravila se zadaju u sledećem formatu:

```
<snort action> <protocol> <IP_1> <PORT_1> <direction> <IP_2> <port_2> (msg:"poruka koja se prikazuje prilikom generisanja upozorenja"; <optional classtype>; <optional snort ID (sid)>; <optional revision (rev) number>;)
```

Snort pravila – nekoliko primera

- Generiši upozorenje za bilo kakav TCP saobraćaj poslat sa adrese 192.168.1.66.
`alert tcp 192.168.1.66 any -> any any (msg:"Saobracaj sa 192.168.1.66");)`
- Generiši upozorenje u slučaju da se u sadržaju paketa nalazi heksadecimalna vrednost 0x90 (instrukcija NOP na arhitekturi x86, moguće prepunjenje bafera).
`alert tcp any any -> any any (msg:"Moguc exploit"; content:"|90|");)`
- Generiši upozorenje samo ako vrednost 0x90 postoji između bajtova 40 i 75 sadržaja paketa.
`alert tcp any any -> any any (msg:"Moguc exploit"; content:"|90|"; offset:40; depth:75;)`
- Generiši upozorenje samo ako je sadržaj TCP paketa veći od 6000 bajtova i vrednost 0x90 postoji između bajtova 40 i 75 sadržaja paketa.
`alert tcp any any -> any any (msg:"Moguc exploit"; content:"|90|"; offset:40; depth:75; dsize: >6000;)`
- Pravilo koje otkriva pakete u kojima su istovremeno postavljeni flegovi SYN i FIN (započinju i završavaju TCP konekciju).
`alert any any -> any any (flags: SF,12; msg: "Moguce SYN FIN skeniranje");)`

Neke tehnike zaobilaženja IDS sistema

- Da se podsetimo:
 - **Rizik** je mogućnost da nastane oštećenje ili gubitak neke informacije, intelektualne svojine, prestiža ili ugleda.
 - **Sigurnost** je proces održavanja prihvatljivog nivoa rizika.
 - Ukoliko je vrednost resursa veća, potrebno je uložiti veća materijalna sredstva u zaštitne mehanizme koji te resurse štite i smanjiti rizik od ugrožavanja poverljivosti, integriteta i dostupnosti resursa.
 - Napadač koji želi da pristupi resursima mora da zaobiđe te mehanizme.
 - Što su resursi značajniji, napadač će takođe uložiti veća materijalna sredstva da uspešno izvrši napad.
 - Apsolutna sigurnost ne postoji, što znači da ne postoji ni jedan savršeni zaštitni mehanizam, uključujući i IDS.

Neke tehnike zaobilaženja IDS sistema

- Postoji veliki broj tehnika za zaobilaženje IDS sistema i nekoliko načina njihove klasifikacije.
- Neke tehnike su opštenamenske a neke upotrebljive za zaobilaženje specifičnih IDS-ova.
- Primeri:
 - Tehnike zaobilaženja IDS sistema zasnovanih na potpisima.
 - Tehnike zaobilaženja IDS sistema sa *Support Vector Machines* klasifikatorom u komponenti za analizu.
- Tehnike zaobilaženja vremenom zastarevaju, zato što proizvođači postaju svesni njihovog postojanja i u svoje proizvode ugrađuju protivmere, tj. tehnike sprečavanja zaobilaženja.
- U ovom izlaganju su ukratko analizirane tri kategorije tehnika zaobilaženja IDS-a:
 - Tehnike zasnovane na **nedostatku konherentnosti** između IDS-a i mreže koje štiti.
 - Tehnike zasnovane na **izvođenju DoS napada na sam IDS**.
 - Tehnike **maskiranja zlonamernog koda**:
 - Šifrovanje, polimorfizam, oligomorfizam i metamorfizam.

Tehnike zasnovane na nedostatku konherentnosti

- Zasnovane su na različitim **konačnim sekvencama fragmenata** koje analiziraju IDS i žrtva.
 - IDS se ne oglašava alarmom ali se napad izvršava.
- Primer:
 - Napadač poznaje topologiju mreže.
 - Napadač menja polje TTL (*Time to Live*) određenih fragmenata.
 - Fragmenti sa izmenjenim TTL poljem:
 - Postoje kada stignu do IDS-a.
 - IDS ne prepoznaje napad zato što ovi fragmenti koji unose varijacije u napad.
 - Nestaju pre nego što stignu do odredišta.
 - Odbacuju se kada prođu IDS (zato što je vrednost TTL polja manja).
 - Originalna sekvenca fragmenata kojom se izvršava napad prosleđuje se žrtvi.

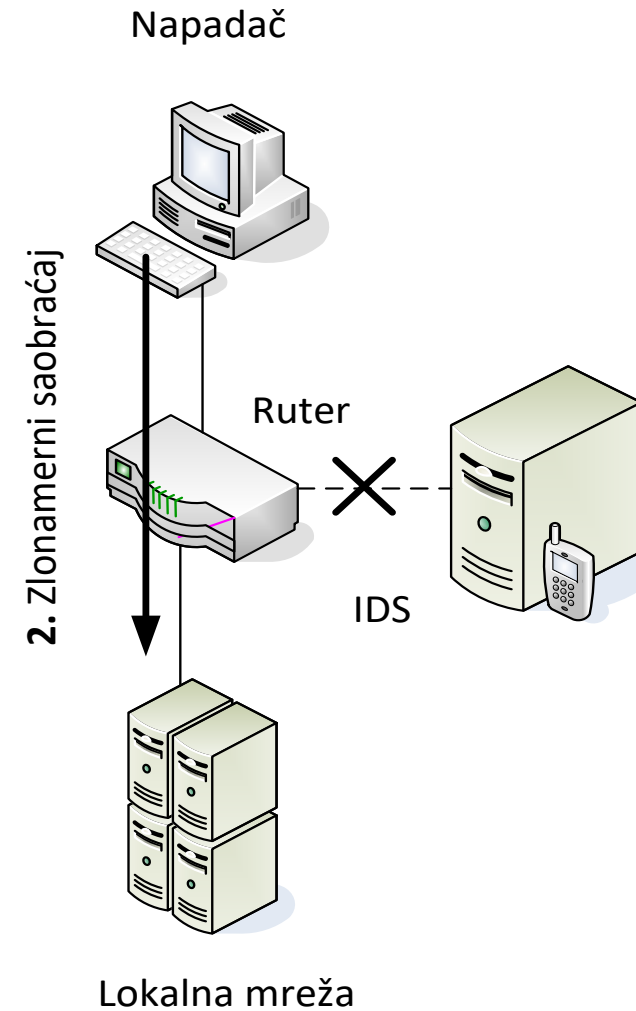
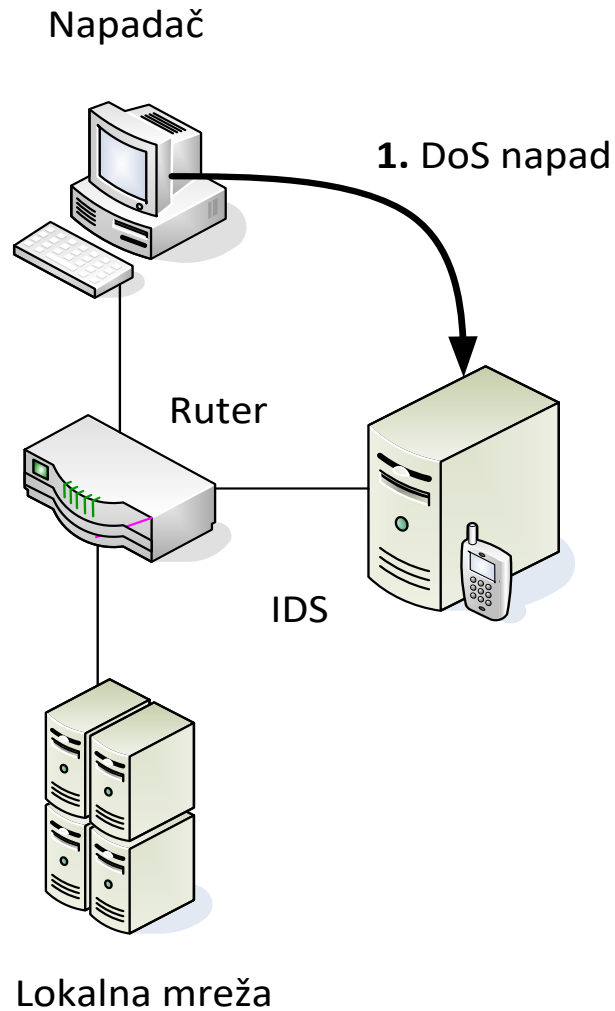
Tehnike zasnovane na nedostatku konherentnosti

- Ove tehnike mogu biti zasnovane i **eksploataciji ranjivosti TCP/IP** skupa protokola.
- Primer: slanje RST paketa sa pogrešnom kontrolnom sumom.
 - Napadač uspostavlja TCP konekciju sa serverom koji IDS nadgleda.
 - Napadač šalje RST paket sa pogrešnom kontrolnom sumom.
 - IDS na osnovu RST paketa zaključuje da je konekcija između napadača i servera prekinuta.
 - IDS prestaje da nadgleda tu konekciju.
 - Server prima RST paket.
 - Server računa kontrolnu sumu.
 - Upoređuje je sa sumom koja se nalazi u zaglavlju primljenog paketa.
 - Pošto se razlikuju, server odbacuje RST paket i nastavlja TCP vezu sa napadačem.
 - Napadač dalje šalje zlonamerne pakete koje IDS neće otkriti jer smatra da je veza prekinuta.

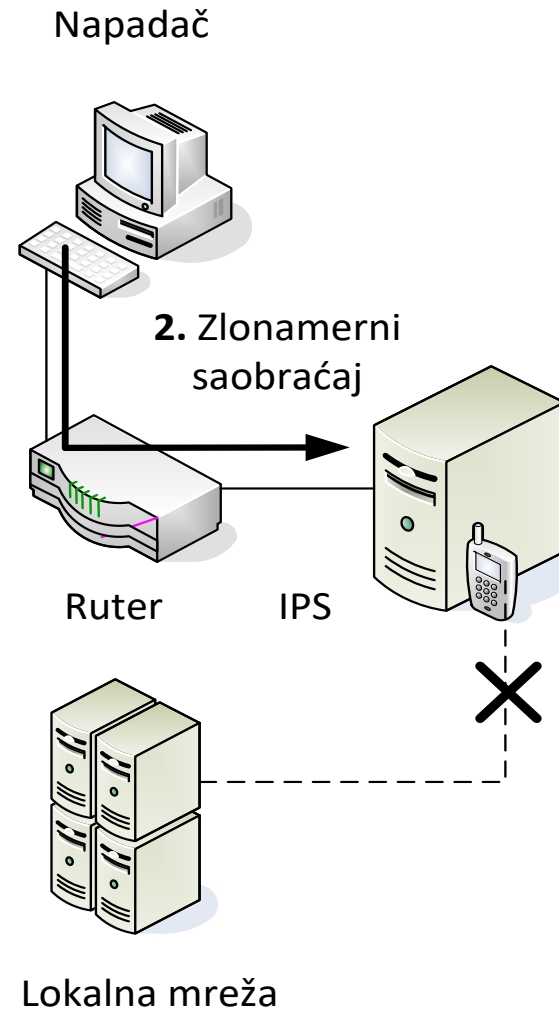
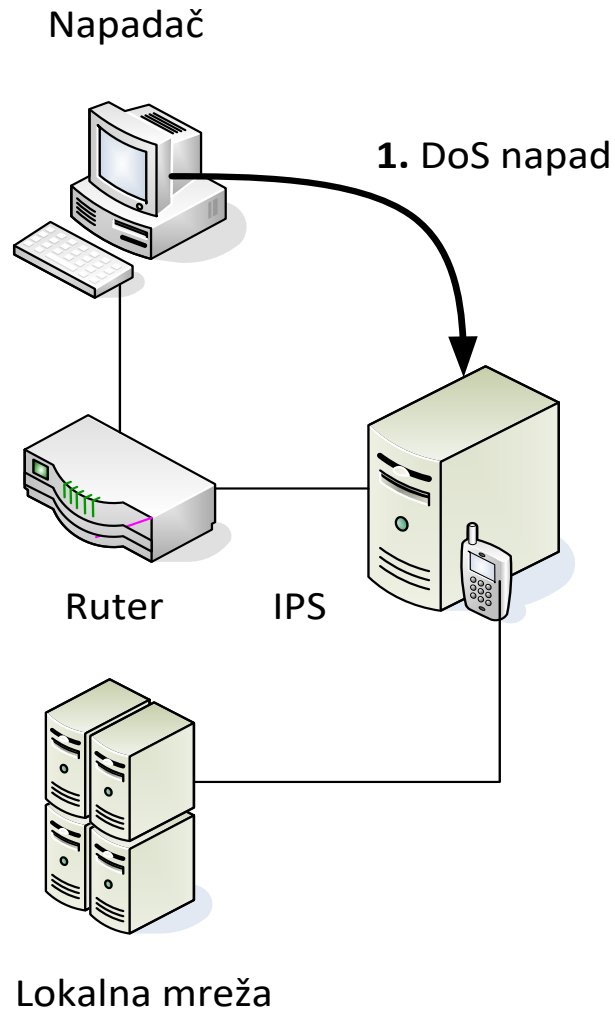
Tehnike zasnovane na izvođenju DoS napada na IDS

- Postoji nekoliko tehnika za izvođenje DoS napada na IDS sisteme.
- Primeri:
 - Preplavlivanje lažnim alarmima (*alert flood*).
 - Neke varijante se mogu iskoristiti za prikrivanje prave prirode napada.
 - Izazivanje redosleda poređenja sa pravila koje najviše opterećuje procesor IDS sistema i usporava algoritam detekcije.
- Posledice DoS napada zavise od toga u kom režimu IDS radi i na koji je način vezan za mrežu.
 - Ako IDS samo nadgleda saobraćaj:
 - Nakon izvođenja DoS napada IDS se ne oglašava alarmom u slučaju napada na mrežu.
 - Mreža ostaje ranjiva dok se ne uklone posledice DoS napada na IDS.
 - Ako IDS radi u preventivnom režimu:
 - Sistem prestaje da opslužuje mrežu.
 - Zlonamerni saobraćaj ne može proći ka zaštićenim računarima u mreži.

Tehnike zasnovane na izvođenju DoS napada na IDS



Tehnike zasnovane na izvođenju DoS napada na IDS



Tehnike maskiranja zlonamernog koda

- **Maskiranje** je tehnika kojom se originalni kod pretvara u:
 - Kod koji zadržava istu funkcionalnost.
 - Njegovo razumevanje je otežano.
- Napadači su počeli da primenjuju ove tehnike kako bi **otežali ili onemogućili detekciju** maskiranog zlonamernog koda.
- U početku je obavljano tehnikama **kompresije** ili **šifrovanja** zlonamernog koda.
- IDS lako može da otkrije modul za dešifrovanje na osnovu potpisa (modul je neophodan).
- Razvoj maskiranja je zbog toga usmeren je u tri pravca:
 - **Oligomorfizam** (generisanje različitih modula za šifrovanje koda odabirom delova iz nekoliko predefisanih šablona)
 - **Polimorfizam** (mutacija kriptografskog modula sa svakom kopijom koda)
 - **Metamorfizam** (mutacija zlonamernog koda).
- Oligomorfni kod se može detektovati na osnovu potpisa (u bazi postoje potpisi svih šablona).
- Oligomorfni i polimorfni kod se mogu otkriti sistemima za detekciju anomalija.

1. D. Pleskonjić, N. Maček, B. Đorđević, M. Carić (2007): Sigurnost računarskih sistema i mreža. Mikro knjiga, Beograd.
2. N. Maček (2015): Detekcija upada mašinskim učenjem / Machine Learning in Intrusion Detection. Zadužbina Andrejević.

Pitanja su dobrodošla.