Bezbjednost i zaštita informacionih sistema

Sistemi za detekciju i prevenciju upada

Prof. dr Nikola Žarić

e-mail: zaric@ucg.ac.me

Pojam upada u sistem

- DžimAnderson: upad u računarski sistem ili mrežu je svaki neovlašćeni pokušaj:
  - pristupa, izmjene ili uništavanja informacija,ili
  - dovođenja sistemau nepouzdano ili neupotrebljivo stanje.
- Drugim riječima, upad je bilo koji skup akcija koji narušava integritet, povjerljivost ili raspoloživost resursa.
- Pokazalo se da zaštita kontrolom pristupa, mrežnom barijerom i softverom za sprječavanje infekcije zlonamjernim programima (virusi, crvi, trojanski konji, špijunski programi) nije dovoljna.7
- **Sistemi za detekciju upada**
- **Sistemi za prevenciju upada**

Sistemi za detekciju upada

- Sistem za detekciju upada provjerava dolazeći (engl. *inbound*) ili odlazeći (engl. *outbound*) saobraćaj i identifikuje sumnjive uzorke koji mogu da indikuju napad na mrežu ili računarski sistem ili da kompromituju sistem.
- Primjeri upada mogu biti izvedeni uz korišćenje dodatnih elemenata ili u cjelini sa:
    - virusom,
    - prekoračenjem bafera,
    - odbijanjem usluge, ili
    - lažiranjem IP adrese.

Sistemi za detekciju upada

- Problem poznat pod imenom prelivanje (prekoračenje) bafera jedan je od zanimljivih primjera koji je sve češće eksploatisan.
- On je najčešće posljedica programerske greške. U okviru zloupotrebe ovog propusta, može se koristiti dodatni kod koji je napravljen da pokrene posebne akcije koje će poslati instrukciju napadnutom računaru da izvrši vrlo štetne akcije kao što su: uništavanje ili izmjenapodataka, otkrivanje poverljivih informacija ili narušavanje funkcionisanja rada računara.
- Napadi prekoračenja bafera nastali su nakon što je u okviru programskog jezika C stvorena takva mogućnost tj. okvir, a programeri i njihove loše prakse ili neznanje stvorilo ranjive tačke
- **Odbrana od ove vrste opasnosti sastoji se u tome da programeri poznaju moguće probleme i da se drže pravila prilikom programiranja.**

Sistemi za detekciju upada

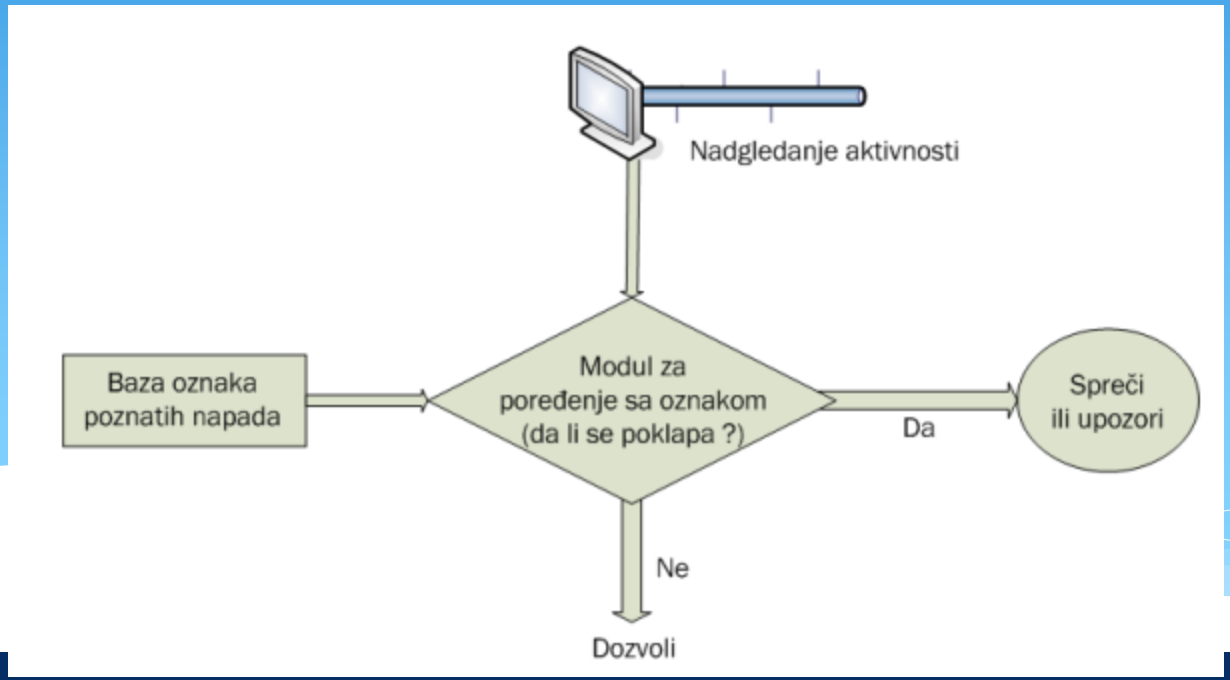
- Jedan poseban slučaj opasnosti koja se pojavljuje je rootkit.
- **Rootkit** je skup alata ili alat koji se sastoji od malih i korisnih programa koji omogućavaju napadaču da ima pristup „root“ korisniku tj. korisniku sa najviše ovlašćenja u sistemu. Drugim riječima, rootkit je skup programa i koda koji omogućava permanentno i konzistentno, neprimjetno prisustvo na kompjuteru. Da bi se zaobišao IDS / IPS softver, postoje dva pristupa: aktivni i pasivni.
- Aktivan pristup se koristi u vrijeme izvršavanja i dizajniran je da se preduprijedi otkrivanje.
- Samo ako neko postane sumnjičiv, pasivni pristup se aktivira iza scene kako bi se potražnja i otkrivanje učinili što težim.

Podjela IDS sistema

- Sistemi za detekciju upada su klasifikovani na više načina, zavisno od kriterijuma za klasifikaciju:
  - šta se detektuje,
  - gdje je IDS sistem smješten,
  - kada otkriva napad, i
  - kako reaguje na napad.
- Kriterijum podjele: šta se detektuje?
  - **detekcija zloupotreba** (engl. *misuse intrusion detection*) - podrazumijeva otkrivanje poznatih napada koje eksploatišu poznate slabosti tj. ranjivosti sistema,
  - **detekcija anomalija** (engl. *anomaly intrusion detection*) - koncentriše na neuobičajenu aktivnost uopšte govoreći, koja može indicirati upad.

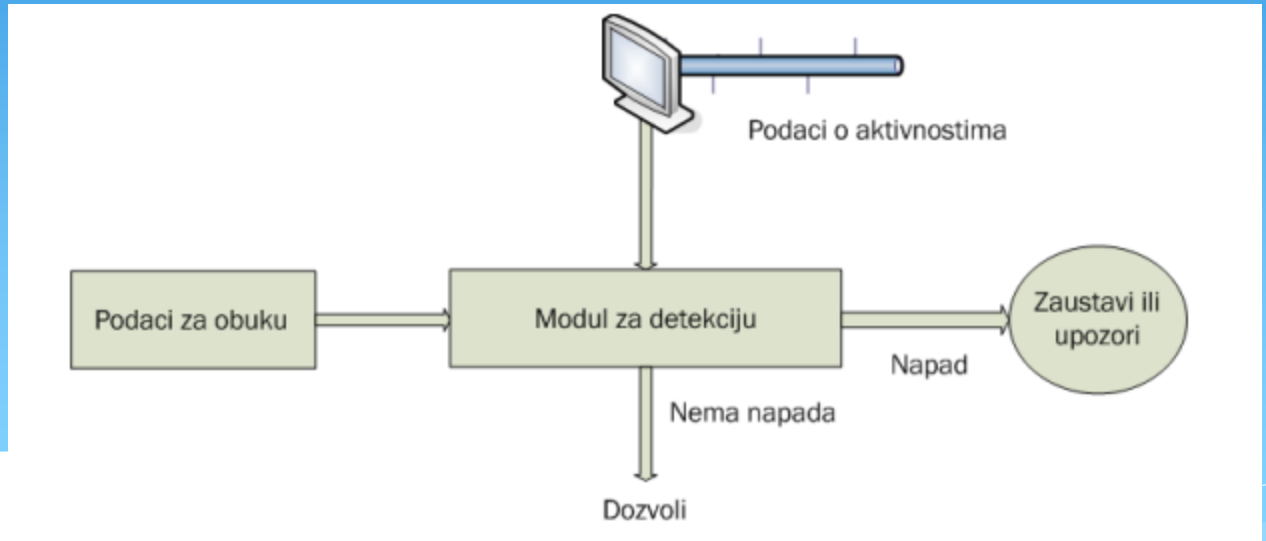
Podjela IDS sistema

- Sistemi za detekciju zloupotreba



Podjela IDS sistema

- Sistemi za detekciju anomalija



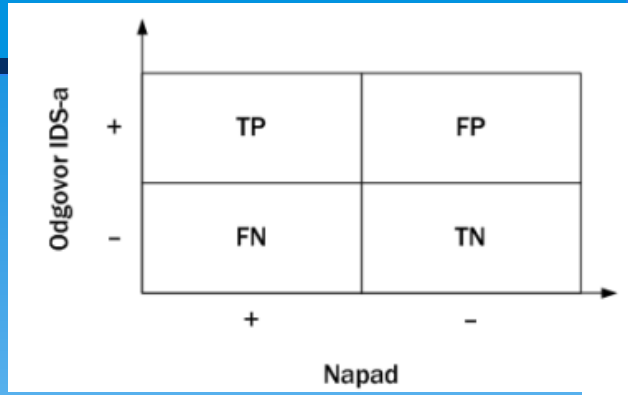
Podjela IDS sistema

- Kriterijum podjele: gdje je sistem smješten?
  - Host bazirani IDS,
  - Mrežno bazirani IDS, i
  - Aplikativno bazirani IDS.
- Kriterijum podjele: kada je napad otkriven?
  - u realnom vremenu (engl. *real time*) i
  - naknadno, tj. nakon dešavanja (engl. *after the fact*, *post-mortem*).
- Kriterijum podjele: reakcija na napad
  - Pasivni
  - Aktivni

Podjela IDS sistema

- Faze odgovora na napad prema Bishopu su sljedeće:
  - priprema (engl. *preparation*),
  - identifikacija (engl. *identification*),
  - ogradjivanje – okruživanje (engl. *containment*),
  - iskorjenjivanje (engl. *eradication*),
  - oporavak (engl. *recovery*),
  - nastavak (engl. *follow-up*).

Teorija IDS sistema



- Osetljivost,
- Određenost, i
- Tačnost.
- Osa nazvana “upad” označava da li se upad zaista dogodio: "+" znači da je zaista postojao upad, dok "-" znači da nije bilo upada.
- Druga osa (odgovor IDS-a) označava da li IDS misli da je detektovao upad (“+”) ili ne (“-”). Kao što je slučaj i u realnom svijetu, ovaj model pokazuje da IDS nije uvijek u pravu.
- Četiri slučaja koji su predstavljeni kvadrantima ove tabele će Vam pomoći da lakše razumijete statistička svojstva IDS-a.

Teorija IDS sistema - Osjetljivost

- Osjetljivost (engl. *sensitivity*) se definiše kao učestanost pravih alarma (engl. *true positive rate*), tj. količnik broja stvarnih upada koje je IDS detektovao (TP) i zbira pravih alarma i propuštenih alarma. Matematički, osjetljivost je izražena na sljedeći način:
  - osjetljivost = TPR = TP / (TP + FN)
- Učestanost propuštenih alarma (engl. *false negative rate*) se definiše kao količnik broja stvarno negativnih i zbira stvarno pozitivnih i lažno negativnih:
  - FNR = FN / (TP + FN) = 1 – TPR = 1 – osjetljivost.
- Osjetljivi IDS-ovi (engl. *sensitive IDSs*) su korisni za identifikovanje napada na područja mreže u kojima se diskriminacija aktivnosti lako može ispraviti ali upad ne smije nikada promaći.

Teorija IDS sistema - Određenost

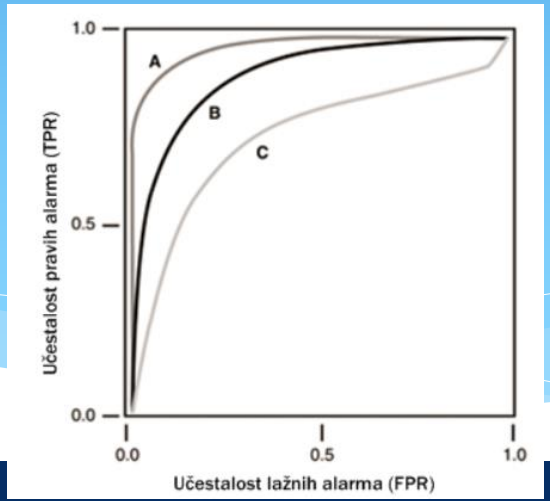
- Matematički, određenost (engl. *specificity*) definiše se kao odnos učestanosti ispravno detektovanih legitimnih aktivnosti, tj. kao količnik ispravno detektovanih legitimnih aktivnosti i zbira stvarno negativnih i lažnih alarma:
  - osjetljivost = TNR = TN / (TN + FP)
- TN je slučaj kada IDS korektno izvještava da nema upada. Do FP dolazi kada IDS pogrešno izvijesti da postoji upad, kada ga u stvarnosti nema. Učestanost lažnih alarma (engl. *False Positive Rate*) određuje se kao:
  - FPR = FP / (TN + FP) = 1 – TNR = 1 – određenost
- IDS-ovi sa visokom određenošću (engl. *specific IDSs*) imaju veliku važnost za administatore mreža. Za ove programe, pozitivni rezultati su korisniji nego negativni rezultati.

Teorija IDS sistema - Tačnost

- Tačnost (engl. *accuracy*) je termin koji obuhvata i određenost i osjetljivost.
- Tačnost je proporcija, tj. odnos svih IDS rezultata (pozitivnih i negativnih) koji su ispravni, tj. korektni.
- Na primjer, može vam zatrebati IDS sa višom tačnošću u nekom području mreže U ovom slučaju vaš Web server je pod stalnim napadom i to će izazvati njegovo zbunjvanje i može dovesti do finansijskog gubitka, ako se server kompromituje. U tom slučaju je potrebno da da se čak i mala anomalija procesira i to automatski jer je nivo saobraćaja veoma veliki.
- U suštini, da bi se postigao najveći nivo osjetljivosti i određenosti, može biti potrebno i kombinovanje slojeva različitih IDS-ova

Teorija IDS sistema - Kriva operativne karakteristike primaoca

- Operativna karakteristika primaoca (engl. *Receiver Operating Characteristic Curves*, *ROC*) je metod grafičkog prikazivanja relacije između osjetljivosti i određenosti. ROC kriva iscrtava odnos stvarno pozitivnih (osetljivost) u odnosu na odnos lažno pozitivnih (1 – određenost). Ovaj grafik služi kao nomogram (grafički prikaz numeračkih relacija, tj. odnosa).



Teorija IDS sistema - Prediktivne vrijednosti

- Prediktivne vrijednosti su predviđanja izvedena iz rapoloživih podataka.
- Prediktivne vrijednosti se dobijaju kombinovanjem prethodne vjerovatnoće (engl. *prior probability*), tj. vrijednosti koja je dobivena na osnovu prethodne praktične primjene IDS-a u drugim mrežama, sa rezultatima IDS sistema koji radi u mreži za koju se prediktivne vrijednosti računaju.
- Mnogi administratori mreže obavljaju analizu rezultata IDS-a na osnovu intuicije, što je pogrešan pristup koji najšešće dovodi do nepreciznih rezultata.

Teorija IDS sistema - Prediktivne vrijednosti

- Odnos mogućnosti
  Prediktivne vrijednosti predstavljaju vjerovatnoću, tj. opisuju mogućnost da do nekog napada dođe.
- Još jedna korisna vrijednost za analizu IDS sistema je odnos dvije vjerovatnoće (engl. *odds*)
  - vrijednost koja pripada intervalu 0 (što znači nikada),
  - beskonačno (što znači, uvijek).
- Matematička veza između verovatnoće i odnosa je sljedeća:
  - odnos = vjerovatnoća / (1 – vjerovatnoća),
  - vjerovatnoća = odnos / (1 + odnos).

Sistemi za sprečavanje upada - IPS

- Mrežna barijera može zaustaviti servis (uslugu) blokirajući određene portove, ali oni mogu učiniti malo da se ocijeni saobraćaj koji koristi dozvoljene (otvorene) portove.
- IDS može ocijeniti, tj. analizitati saobraćaj koji prolazi ove otvorene portove, ali ga ne može zaustaviti.
- IPS može proaktivno blokirati napade.
- IPS sistemi sprečavaju poznate napade; nove, nepoznate vrste napada je potrebno prvo identifikovati i analizirati i na osnovu toga kreirati potpis, tj. oznaku koja će biti dodana u bazu IPS sistema kako bi se omogućila detekcija napada.

Sistemi za sprečavanje upada - IPS

- IPS sistemi mog da uključuju algoritme za detekciju napada na osnovu definisanih sigurnosnih politika i anomalija u sistemu.
- Spečavanje detektovanih napada se najčešće svodi na prekidanje konekcije sa onih adresa sa ojih su primijećene maliciozne aktivnosti.
- Znači, osnovne funkcije IPS sistema su sljedeće:
  - identifikacija neautoriziranih aktivnosti na osnovu potpisa,
  - identifikacija neautoriziranih aktivnosti na osnovu detektovanih anomalija,
  - vođenje evidencije i/ili slanje upozorenja administratorima zaduženim za sigurnost u realnom vremenu,
  - prikupljanje forenzičkih podataka o detektovanim napadima,
  - sprječavanje napada.

Sistemi za sprečavanje upada - IPS

- Neki od pristupa na kojima rade IPS sistemi su sledeći:
  - Softversko bazirani heuristički pristup - slićan IDS sistemima
  - Sandbox pristup
  - Hibridni pristup
  - Pristup baziran na zaštiti pomoću jezgra
- IPS sistemi se dijele na dva osnovna tipa:
  - Host bazirani IPS (engl. *host based IPS*, *HIPS*)
  - Mrežno bazirani IPS (engl. *network based IPS*, *NIPS*)

Sistemi za sprečavanje upada - IPS

- IPS sistemi, kao i sve druge sigurnosne tehnologije, imaju svoje prednosti i nedostatke. Neke od prednosti HIPS sistema su:
  - zaštita od takozvanih "*zero day*" napada na sistem,
  - smanjene obaveze zaposlenih koji su odgovorni za sigurnost (na primjer, upravljanje zakrpama),
  - smanjenje troškova održavanja sistema i
  - mogućnost implementacije u aplikacije koje se razvijaju.

Sistemi za sprečavanje upada - IPS

- Nedostaci HIPS sistema su sljedeći:
  - troškovi implementacije (sistem zahtijeva agenta za svaku radnu stanicu),
  - relativno dug period implementacije i podešavanja (tj. obučavanja),
  - izazivanje problema u radu aplikacija (ukoliko je sistem loše konfigurisan),
  - neophodnost testiranja svake nove aplikacije u interakciji sa HIPS sistemom prije uvođenja,
  - ne čiste infekcije do kojih je već došlo.

  .

Sistemi za sprečavanje upada - IPS

- Zahtevi za efikasnu prevenciju:
  - Nepobitna tačnost detekcije
  - Otpornost na nove napade
  - Raspoložost
  - Malo vreme čekanja tj. Kašnjenje
  - Napredno rukovanje alarmima i mogućnost naknadne analize