



едуцентар

## Видови системи за детекција на наметнувања



# Intrusion Detection Systems (IDS)

## (Систем за детекција на наметнување)

Заедно со firewall-ите (огнените ѕидови), Системите за детекција на наметнувања (IDS) се главна компонента во денешно време во светот на сигурносни системи. Улогата на IDS е да се обиде да фати во стапица присуство на некој хакер во загрошена мрежа, да елиминира секаков вид на прекршок или злоупотреба што е произлезено од присуството на хакерот и архивирање на постапките во вид на каталог за да се избегнат слични напади во иднина.

Наметнувањето (Intrusion) е технички дефинирано како: "обид од страна на неавторизиран ентитет да ја загрози автентичноста, интегритетот и доверливоста (CIA = Confidentiality, Integrity and Availability) на некој ресурс.

Наметнувањето ги содржи следните видови на напади:

1. Оштетување на осетливи информации во внатрешна мрежа
2. Присвојување на доверливи и лични информации
3. Потиснати функции и ресурси достапни на можни законски корисници

IDS се потребни за да спречат проблеми кои настануваат од некој напад. Поправањето на штетата направена од страна на напаѓачот и легалните постапки можат да бидат многу скапи и да одземаат многу време за разлика од тоа да се детектира присуството на напаѓачот и негово одстранување во рани фази. IDS создаваат многу добар лог за намерите и модификациите од страна на разни напаѓачи кој може да се искористи за спречување и надмудрување на можни напади во иднината. Затоа способностите на денешните детекции на наметнување снабдуваат некоја организација со добар ресурс за целосна анализа на сигурност. Прашањето каков вид на IDS да се имплементира зависи од големината и опсегот на внатрешната мрежа на организацијата, количините на доверливи информации што таа организација ги одржува и т.н.

Од време на време, напаѓачите ќе успеат да загрозат други сигурносни мерки, како криптографија, firewall-и и др. Клучно е да знаењето за ваквите загрозувања веднаш дојде до администраторите. Таквите задачи лесно можат да се завршат со помош на IDS. Немарноста на администраторите претставува сериозен проблем во мрежната сигурност. Примена на IDS може да помогне на администраторите да приметат некаква пропуштена слабост или експлоатација што некој напаѓач може да ја изврши. Некои од најпознати користени IDS се: [Snort](#), [Cisco Secure IDS](#), [Dragon Sensor E-Trust IDS](#), [Audit-Guard](#), [Symantec](#) и [Tripwire Snort](#).

## Видови на IDS

IDS системите спаѓаат во многу различни категории зависно од нивните функции и архитектура. Секој вид си има свои специјализирани функции. Организацијата што посакува да имплементира IDS обично проаѓа низ многу проверки и ревизии во врска со нивните сигурносни потреби и побарувачки пред да изберат прикладен IDS. Обично, IDS системите се класифицирани во следните категории:

1. Host-based intrusion detection systems (HIDS)
2. Network-based intrusion detection systems (NIDS)
3. Intrusion prevention systems (IPS)

## Хост-базирани Intrusion Detection Systems (HIDS)

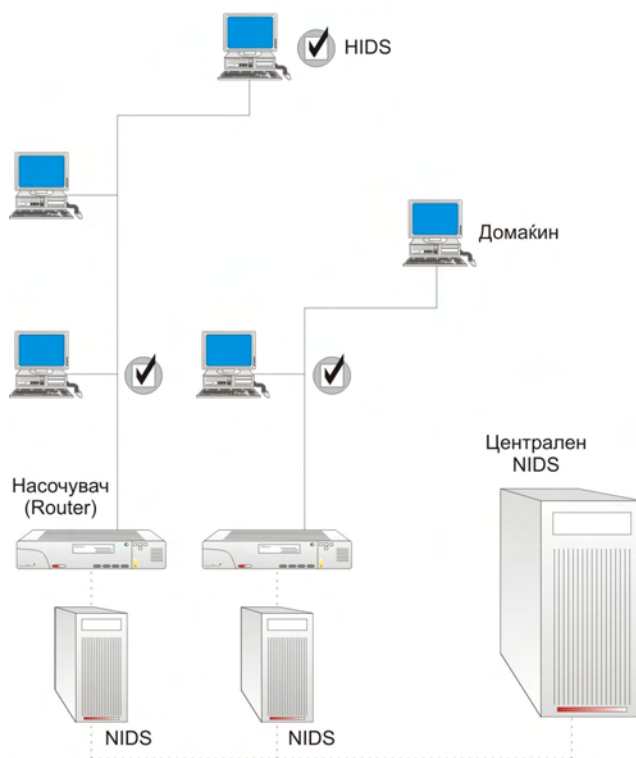
Хост-базирани IDS системи служат за надзор, детекција и одговор на активност и напади врз даден хост (домаќин). Во повеќе случаи, напаѓачите целат на поединечни системи во големи мрежи кои имаат доверливи информации. Тие често ќе се обидат да инсталираат програми што скенираат и други слабости што можат да пратат некоја активност на корисник на некој поединечен хост.

Хост-базиран IDS им овозможува на организации или на индивидуални сопственици на хост во мрежа да се заштитат против или детектираат потенцијални напаѓачи кои можат да откријат сигурносни пропусти или експлоатираат други ранливости или слабости. Некои HIDS алатки овозможуваат менаџмент на политики, статистичка анализа и истрага (форензика) на податоци на дадено хост ниво.

HIDS се најдобро искористени кога напаѓачот се обидува да пристапи до посебни фајлови или други услуги кои се наоѓаат на хост компјутер. Во повеќето случаи, HIDS се интегрирани во самиот оперативен систем (ОС). Бидејќи напаѓачите главно се фокусираат на слабости кај оперативните системи за да навлезат во хостови, таквите имплементации на HIDS се многу поволни.

Од поодамна, многу HIDS биле инсталирани на самите хостови, затоа што ни една единка не можела да биде достапна за големи мејнфрејми (кои барале поголема сигурност) во брзо и ефикасно време. Ваквиот метод предизвикувал сигурносна препрека. Напаѓач, кој ќе успее да го надитри IDS-от и другите сигурносни заштити би можел лесно да го исклучи системот (IDS) за понатамошни злонамерни постапки. Таквите непредности се надминуваат кога IDS-от е физички одделен од самите хостови. Кога одиме на персонални компјутери и поевтини хардверски делови, одделни единки за имплементација на IDS се добар избор.

## Централизиран IDS



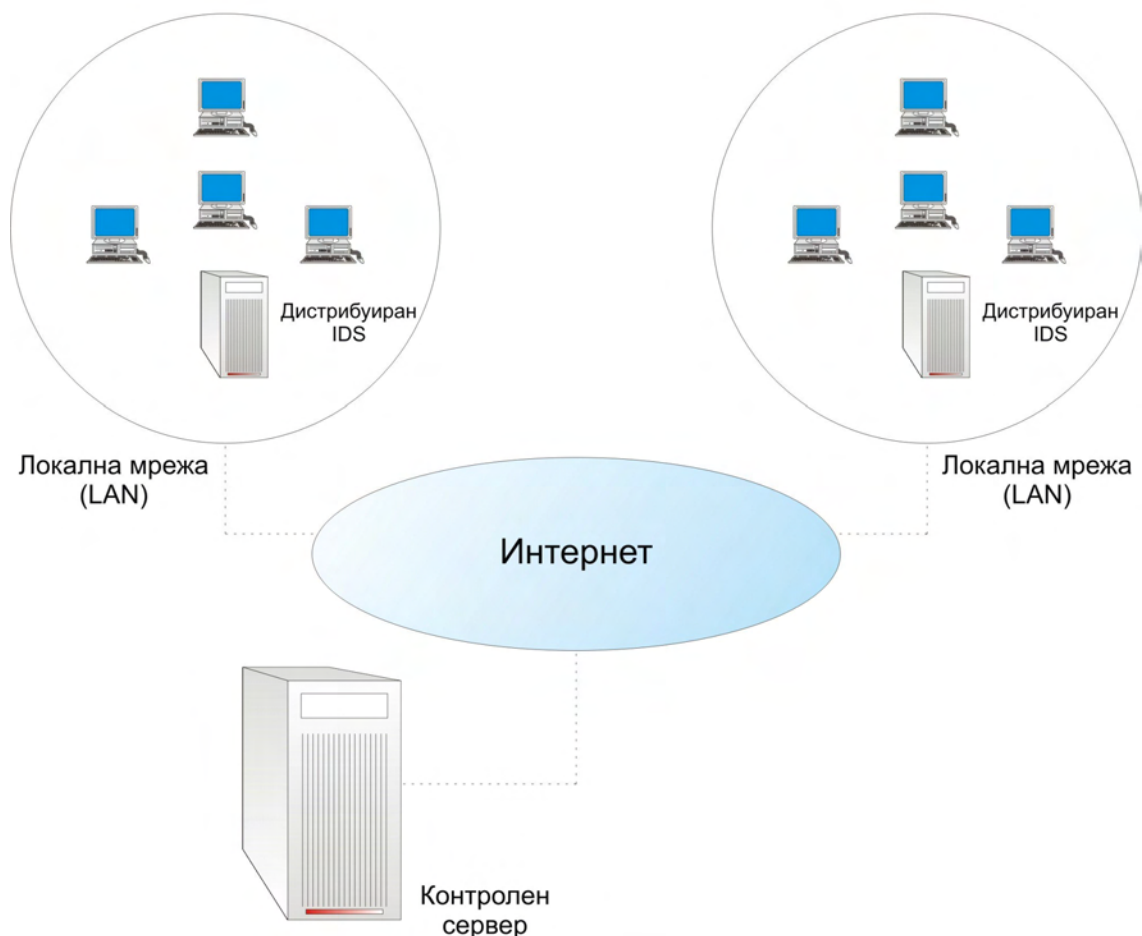
## Мрежно-базирани Intrusion Detection Systems (NIDS)

Мрежно-базирани IDS заробуваат (capture) мрежен сообраќај на целата мрежа или од поголемиот дел од мрежата за нивните операции за детекција на неовластен пристап. Во повеќето случаи овие системи работат како "снифери" на пакети (packet sniffers) кои го "прочешлуваат" сообраќајот што доаѓа и користат посебна метрика за да заклучи дали мрежата е компрометирана.

Многу интернет и други протоколи, како TCP/IP, NetBEUI, XNS и т.н. кои се справуваат со пораки помеѓу внатрешни и надворешни мрежи се ранливи на напади и мораат да зависат од додатни средства поради детекција на злонамерни настани. Обично IDS-те имаат тешкотии во работа со енкриптирани информации и сообраќај што доаѓа од виртуелно приватни мрежи. Брзината (над 1 Gbps) е лимитиран фактор иако најновите изданија на IDS системите имаат можност да работат многу побрзо. Слика 2. претставува репрезентација на HIDS и NIDS употребени на мрежи.

NIDS-ите можат да бидат централизирани и дистрибуирани. Од претходната слика можевте да видите како изгледа централизиран NIDS. Дистрибуираните NIDS работат со нивни агенти (клиенти) кои можат да се наоѓаат секаде во светот и да дават извештај до главниот контролен сервер.

### Дистрибуиран IDS



## Intrusion Prevention Systems (IPS)

IPS системите се софистицирана класа од имплементација на мрежна сигурност кои не само што имаат способност да го детектираат присуството на напаѓачот и неговите постапки туку и да го оневозможи (спречи) да изврши било каков напад.

IPS-ите во нив вклучуваат хармоничен збир од firewall технологија и IDS технологија сè во едно. Можат да се сметаат за успешна интеграција од двете сигурносни технологии (IDS и Firewall) за повисока и поширока сигурносна мерка. Бидејќи IPS-ите се комбинација од сите нивоа на firewall и IDS технологии, често завршуваме со системи кои можат да оперираат на сите нивоа од мрежниот стог(stack). Реализацијата на IPS врз ефикасноста може да биде макотрпен процес. Компаниите треба прво да ги проценат нивните побарувачки и слабости пред да се решат за едно вакво сигурносно решение. IPS-ите понекогаш и неможат да бидат толку брзи и енергични како некои од конвенционалните firewall-и и IDS-и. Поради оваа причина, IPS не е прикладно решение за оние кои имаат потреба од голема брзина и обработување. IPS системите се во константна област на истражување и можат да бидат од голема побарувачка во иднината.