Intrusion Detection Systems

xor cx, [59507] push word [bx] mov ax, [bp-4] sub [si+2], bx not byte [bp+di] add [bx+si+2], dxxor cx, [59507] push word
push ax xor ax, bx mov rsi, rsp mov rdi, 1 mov rdx, 8 call write push ax xor ax, bx mov rsi, rsp mov rdi, 1 mov rdx, 8 call w
mov al, [bx][si] mov al, [bx][di] mov al, [bp][si] mov al, [bp][di] mov al, [bx][si] mov al, [bx][di] mov al, [bp][si] mov al, [bp]

By Даме Јованоски
badc0re

Содржина

Вовед

Денес не постои 100% сигурност, но сепак постои шанса да се намали ризикот од неовластен пристап на некое лице во нашата компјутерска мрежа. Тоа можеме да го направеме со воведување на уреди кои всушност ќе го детектираат и исто така реагираат на одреден сомнителен напад. Тие уреди се IDS(Intrusion Detection Systems) т.е систем за детекција на неовластен пристап кои можат да помогнат во спречувањето на овие неовластени упади. Без разлика дали ние имаме некој Web сервер или пак сервер за администрација на некоја локална мрежа, IDS можат да детектираат малициозни напади базирани према пропустите коишто ги имаат самите страни или пропустите на сотверскиот дел на еден оперативен систем како дел од еден сервер. Тоа значи дека имаме Web базирани и апликатино базирани напади. Правилата коишто се дефинираат за IDS се дефинираат од страна на експерти кои имаат добро познавање за типот на нападот, карактеристиките и целта на нападот со што дефинираат таканаречени правила со цел спречување на малициозните корисници од добивање на неовластен пристап до одредена локална мрежа. Во продолжение ќе бидат објаснати карактеристиките на IDS, типовите на напад на истите, алгоритминте коишто се користат и тн.

1. Што претставува IDS?

IDS (Intrusion Detection Systems) претставуваат системи кои имаат за цел да детектираат неовластен пристап во компјутеската мрежа. Како неовластен пристап се подразбира обидот да се пристапи, компромизира или направи штета на уреди кои што се поврзани на една компјутерска мрежа.

Типови на неовластен пристап се:

- Eavesdropping
- Data Modification
- Identity Spoofing (IP Address Spoofing)
- Password-Based напад
- Denial-of-Service напад
- Man-in-the-Middle напад
- Compromised-Key напад
- Sniffer напад
- Application-Layer напад

IDS е high-tech е еквивалент на алармот против провалување, којшто е конфигуриран да го следи протокот на информации на gateway-от, непријателски дејности или некој веќе идентификуван напаѓач. IDS е специализирана алатка која знае како да ги спои и обработи акциите и протокот на податоци на мрежата или хостот. Во податоците кои што ги анализира IDS се вклучуваат мрежите пакети кои што влегуваат и излегуваат во една мрежа како и содржината на лог фајлотивите кои што се креираат од страна на рутерите, firewall-ите и серверите. Принципот на работа на овие системи е таков што тие имаат одредена база на податоци во која се зачувани одредени информации за одреден напад, додека начинот на детекција се базира на споредба на овие информации (од базата) со тековниот напад. Доколку се детектира напад, IDS предизвикува вклучување на алармот и некои предупредувања, следен чекор е активирање на автоматизирани акции како исклучување на интернетот или следење и собирање на информации за идентификација и собирање на докази на напаѓачот или серверот активира повратни напади со цел детекција на напаѓачот(launching back-traces).

2. Кои се причините за нивно воведување?

По аналогија, улогата на IDS во компјутерската мрежа е иста како и работата на антивирусот на еден компјутески систем да спречи одредени фајлови со малициозни содржини, разликата е во тоа што IDS ги детектира малициозните пакети според нивните ознаки (*virus signatures)* деловите кои што се исти како и во базата на податоци или ги детектира можните акции на малициозниот софтвер (во завнисност од нивното однесување).

intrusion detection се мисли на детекција на unauthorized use of или напад на систем или мрежа. Како и firewall-ите, IDS можат да бидат софтверски апликација или комбинација на софтвер и хардвер во вид на самостоен IDS уред (пример десктоп компјутер преинсталиран и преконфигуриран со цел користење како IDS\firewall). На истите уреди можат да работат и firewall, проксите, операторите на сервиси, некои додатни сензори и управувачи како дел од IDS. IDS неможеме да ги користиме и добиеме оптималните резултати доколку ги користиме како дел од истиот уред на којшто имаме некој сервер, firewall и слично. Овие системи се исто така корисни за детектирање и на напади од корисниците кои се дел од самата компјутерска мрежа, како и на детектирање на одредени престапи при пристап до одредени ресурси со одредени пермисии кои што не му дозволуваат нивно менување или користење.

Во пракса, компаниите имаат во мрежата имаат комбинација на апликација или хардверски IDS како дел од сервер/клиент со цел нивна обзервација на настаните што се случуваат во мрежата како и прегледување на комуникацијата на апликациско ниво.
Освен пристапот кој претходно го спомавме т.е прегледот на потписи (signature detection) друг пристап е детекција на аномалии(*anomaly detection)*. Овој начин на пристап користи одредени дефинирани или предефинирани правила за нормална и неправилната(abnormal) комуникација на системот и нивна обзервација доколку настанат. За некои аномалии IDS имплементира кориснички профили(user profiles). Овие профили ги дефинираат границите на нормалната активност и тие се направени користејќи семплирање(sampling), пристап преку одредени дефинирани правила(rule-base approaches), или neural networks.

3. Типовите на IDS.

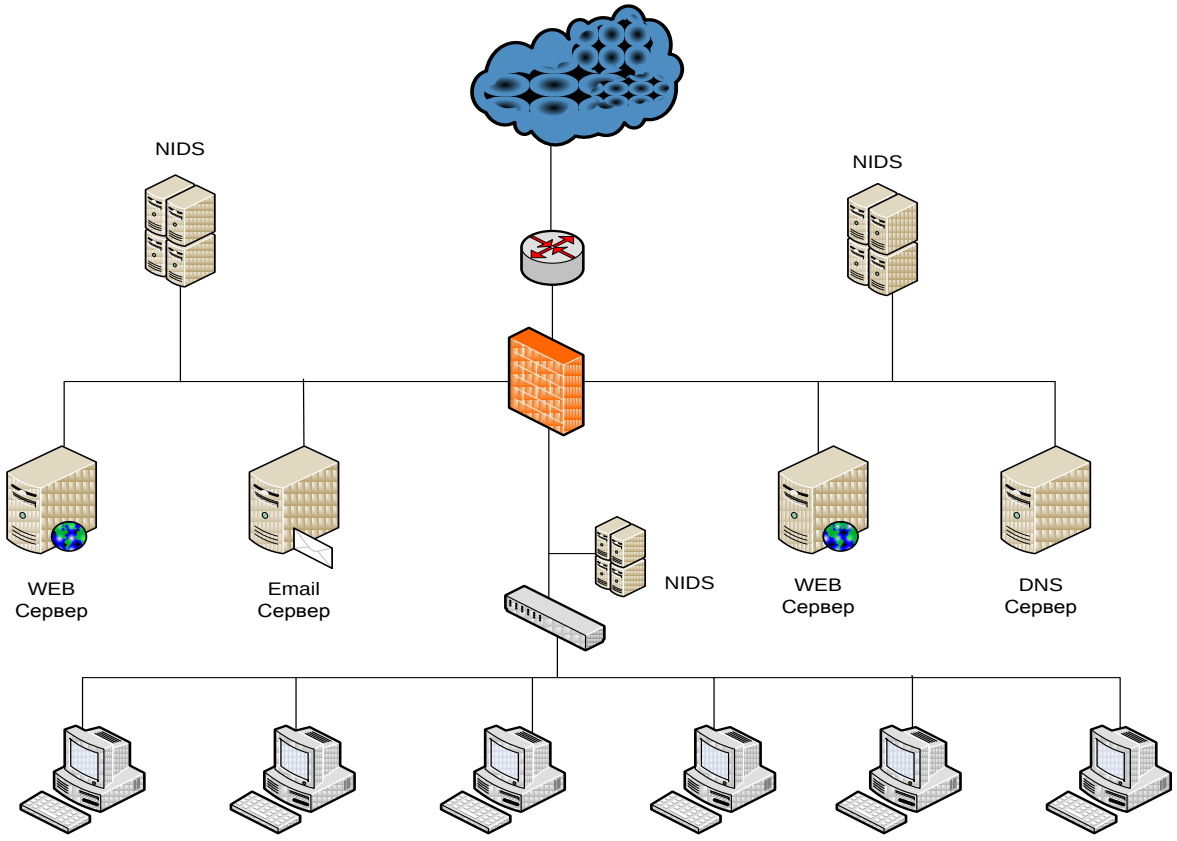
IDS се класифицирани према нивната функционалност и улога во мрежата и според тоа тие се поделени во три главни категории и тоа:

- Мрежно базирани системи за детекција на престап (Network-based intrusion detection system (NIDS))
- Хост базирани системи за детекција на престап (Host-based intrusion detection system (HIDS))
- Дистибуирани системи за детекција на престап (Distributed intrusion detection system

2.1 Мрежно базирани системи за детекција на престап (Network-based intrusion detection system (NIDS))

Како што кажува и самото име мрежни базираните IDS се користат за обзервација на мрежата од перспектива од кадешто тие се вметнати(приклучени). Попрецизно кажано, врши обзеврација на целата мрежа и сите нејзини мрежни сегменти. Се подразбира доколку мрежната карта на компјутерите во мрежата работи во nonpromiscuous мод. Користењето на

овој мод подразбира, само пакетите за точно дефинираната мрежна карта со нејзината MAC адреса ќе бидат сместени во стекот за анализирање. NIDS доколку користи promiscuous мод за обзервација на мрежниот сообраќај ги анализира пакетите кои не се наменети за нејзината MAC адреса. Користењето на овој мод, NIDS може да ја преслушкува(eavesdrop) целата комуникација од мрежата. NIDS треба да биде конектиран на локалниот SPAN(Switched Port Analyzer) порт на локалниоте switch connected to either a span port on your local switch, или на мрежниот таб(делот каде што се конфигурира) со цел дуплицирање на сообраќајот. И според ова заклучуваме дека целта на NIDS-вата NIC картичка во promiscuous mode е заштита на мрежата.

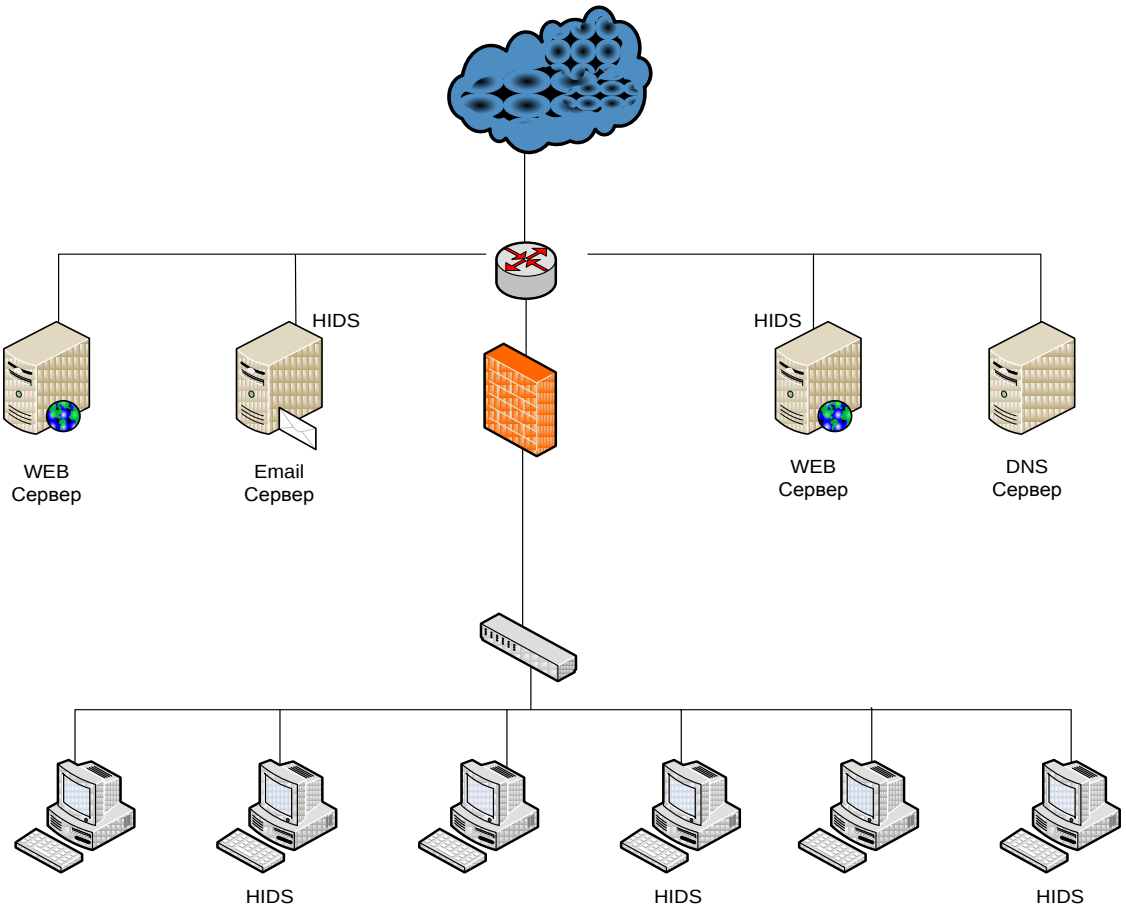


Слика 1.1

На сликата 1.1 ни е прикажано сценарио на користење на три NIDS.Тие се поставени на со цел да вршат мониторинг на мрежниот сообраќај на сите уреди во мрежата. Оваа конфигурација претставува стандардна мрежана топологија каде што стратешки се поставени IDS уредите со цел секоја од подмрежните да биде под обзевација, така што и приватниот и јавниот дел од мрежата е заштитена и овозможува детекција на експлоити со цел да се спречи пенетрирација на напаѓачот во приватните делови.Оваа употреба на повеќе NIDS уреди во мрежата е пример за defense-in-depth безбедностна архитектура.

2.2 Хост базирани системи за детекција на престап (Host-based intrusion detection system (HIDS))

HIDS се разликуваат од NIDS заради две причини. HIDS го штити само делот на хостот којшто и овозможува функционалност на мрежата, и таа под дефолт работи во nonpromiscuous мод. Nonpromiscuous мод на управување може да има предност во некои случаи затоа што некои NIC немаат опција да работат во promiscuous мод. Исто така promiscuous мод може да биде подржани за послаби конфигурации на хостови. Поради тоа што овие системе се користат за обзервација на хостот тие исто така ракуваат со сите додатни информации како додатни локални инфромации(additional local information) со безбедостни импликации ,вкучувајќи ги и системските повици, системски модификации на фајловивите, и системски логови. Во комбинација со мрежните комуникации, со овој начин на ID се овозможува податоците робусно да се пасираат доколку е потребно да се изврши пребарување на одредени безбедностни настани (security events). Друга предност на HIDS е можноста да се овозможи дефинирање на множество на правила за секој индивидуален хост. На пример, нас не ни е поттребно да користиме множество за правила за одреден хост кој ке ни овозможува детектирање на DNS експлоити на хост којшто не користи DNS (Domain Name Services), т.е се редуцира бројот на постоечки правила со кои се зголемуваат перформансите и користењето на процесорот.

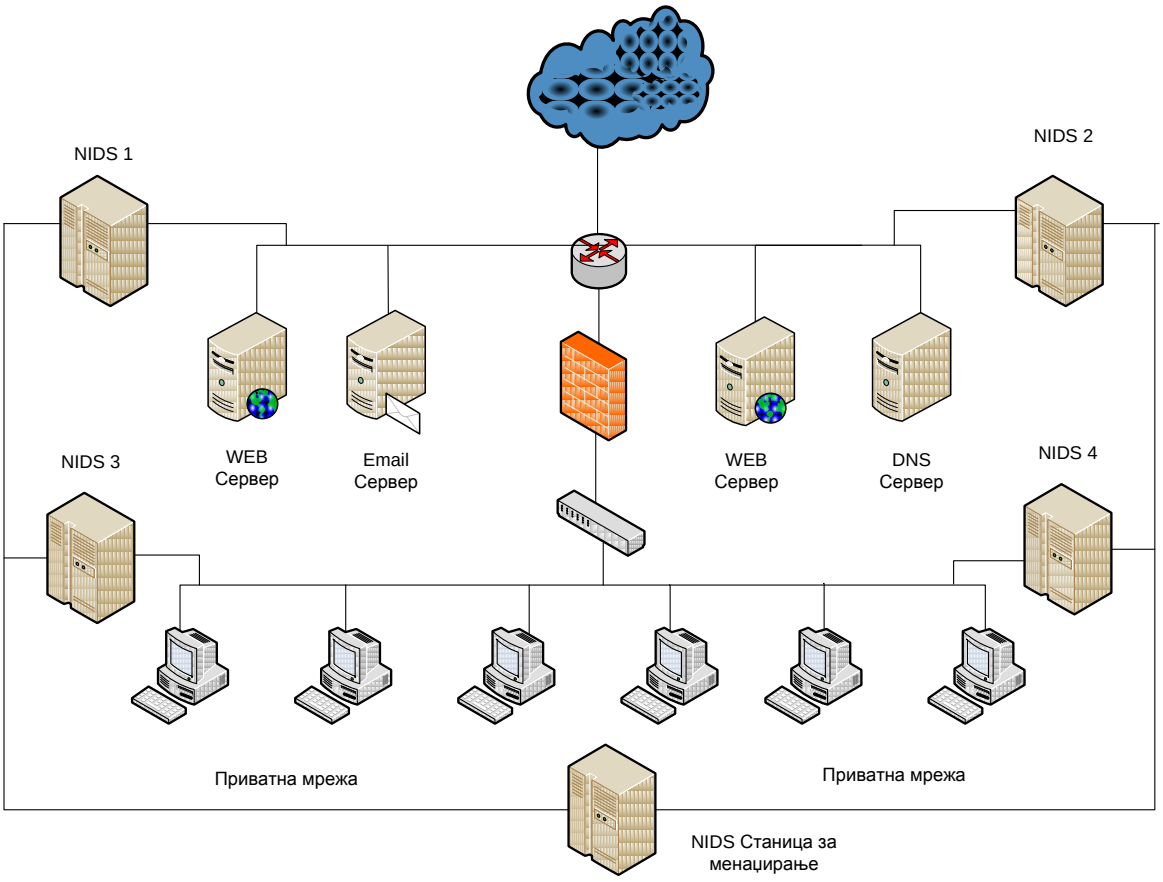


Слика 1.2

На сликата 2 ни е прикажано користење на HIDS, конфигурани на серверски и кориснички компјутери. Од претходното кажано, множеството правила за HIDS на mail серверот се кастомизирани(customized) да го штитат од експлоитите наменети за ваквиот тип на сервер, додека за Web серверот множество правила за Web експлоити. При инсталацијата може да се одбере кој тип на множество правила да биде употребен во зависност од тоа каков сервер користиме.

2.3 Дистибуирани системи за детекција на престап (Distributed intrusion detection system

Стандардните DIDS функционираат користејќи Manager/Probe архитектура (probe – удреди кои служат за сканирање на мрежата и доловување на пакети) т.е архитектура користејќи слоеви. Сензорот за детекции на NIDS користат далечинско лоцирање и тие креираат логови, и истите ги испраќаат до базата за менаџирање. Логовите креирани при напад на мрежата се периодично прикачуваат до центарот за нивно менаџирање користејќи база на податоци.Секое правило за секој сензор си има свои дефинирани карактеристики, така што при детекција на некој напад, системот за информирање(messaging system) лоциран на базата за менаџирање ќе биде употребено за да се информира IDS администраторот.



Слика 1.3

На сликата 1.3 е прикажано DIDS составено од четири сензори и централна станица за менаџирање. Сензорите NIDS 1 и NIDS 2 користат прикриен promiscuous мод со цел да се заштитат јавните сервери. Сензорите NIDS 3 и NIDS 4 го штитат корисничкиот дел во trusted computing зоната. Комуникацијата помеѓу сензорите и станицата за менаџирање може да се оствари преку приватна мрежа или може да се користи истата инфаструктура (да не се создава приватна мрежа). Кога се користи веќе постоечката мрежа за менаџирање таа треба да се енкриптира или да се конфигурира VPN заради безбедност.

DIDS зависат од комплексноста на мрежата, исто така функционалноста варира во зависност од тоа кој производител на DIDS ќе се употреби. Во DIDS индивидуалните сензори можат да бидат NIDS, HIDS, или комбинација на двете, така што тие можат да функционираат во promiscuous мод или nonpromiscuous мод.

3 Како IDS функционираат?

Како што преходно ги претставивме видовите на IDS и нивната архитектура во една компјутерска мрежа ќе дефинираме на кој начин овие системи работат. Најпрвин ќе треба да разбереме што фсушност овие системи обзервираат во мрежата. Во зависност од тоа што ќе влези(input) во мрежата зависи од тоа што излез и каков резултат на тоа ќе добиеме од страна на IDS, затоа и постојат повеќе видови на IDS. Имаме три видови на IDS во зависност од протокот на инфомации во мрежата т.е:

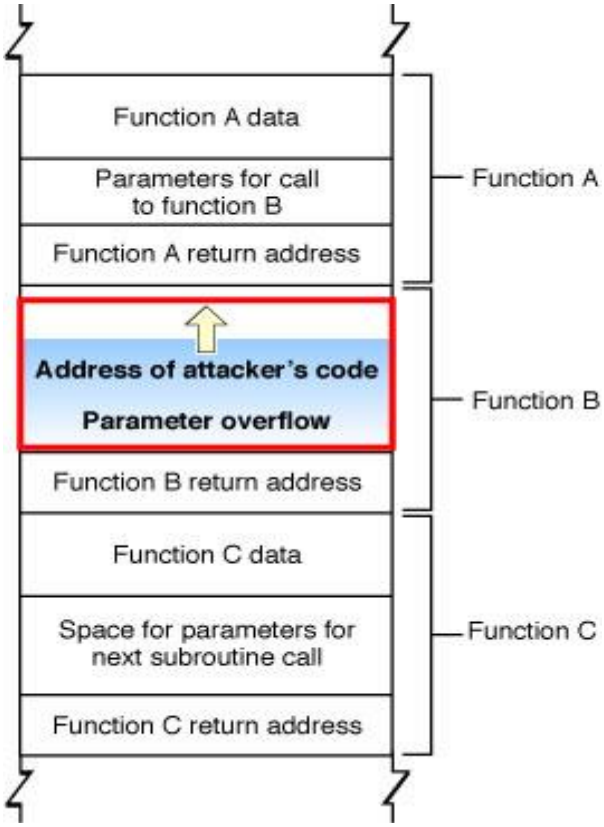
- Апликациско-базирани према инфромаците како податочениот проток (Application-specific information such as correct application data flow)
- Хост-базирани со проток на податоци: системски повици, локални лог содржини или пермисии на фајлови.Host-specific information such as system calls used, local log content, and file system permissions
- Мрежно-базирани со проток на податоци према пакетите кои се праќаат во мрежата. information such as the contents of packets on the wire

DIDS можат да ги имаат карактеристиките на сите овие типови, но сепак зависи кој тип на ID ќе биде искористен и какви далечински сензори има. IDS нивниот начин на функционирање може да варира во зависност од тоа каков начин на прибирање на податоците користат, на пример packet sniffing (воглавно се користи во promiscuous мод за да ги собира податоците најмногу што е можно), пасирање на логови(log parsing) за локалните системски и апликациски логови, преглед на системски повици (system call watching) во kernel со цел да се регулира како апликациите реагираат на овие повици, и системско набљудување на фајловите(file system watching) со цел детектирање на обидите за промена на пермисиите. Кога IDS ќе ги собере податоците од мрежата користи одредени техники за да најде дали има обид за неовластен пристап.
Реакцијата на IDS доколку детектира некој напад може да биде : пасивна(која може да генерира предупредување или лог но не прави никакви манипулации со мрежниот

сообрајќај) и активна(за разлика од пасивната овој тип прави манипулации со мрежата праќа одредени паките за да ги прекини TCP конекциите и истите може да ги блокира).

4 Причини и резулатати од неовластен пристап.

Како резултат на неовластен пристап на одреден компјутер од локалната мрежа може да биде и појавата на Blue Screen of Death, којашто се појавува поради можноста на buffer overflow напад.Секој настан(event) којшто се појавува на нашиот компјутер треба да се пријави до систем администраторот. Денес buffer overflow нападите опфаќаат најголем процент од сигурностните пропусти коишто можат да бидат искористени за пристап до компјутер на одредена локална мрежа. Ваквиот тип на пропусти се резултат на непрофесионалноста на програмерите, кои не го проверуваат дали на резервираното место(buffer) за внесување на карактери(дали при логирање или креирање на некој нов фајл) не ги проверува границите на ограниченият број на карактери. Експлоитите (престставуваат пропусти кои можат да бидат искористени за добивање на пристап на некој компјутер) можат да бидат софтверски и експлоити на оперативниот систем.



Слика 2

Начинот на којшто функционираат овој тип на пропусти е тоа што се внесуваат поголем број на карактери од дозволениот со што се дозволува на напаѓачот да го контролира извршувањето на инструкциите(тие се извршуваат со користење на EIP- instruction pointer register). Со добивање на

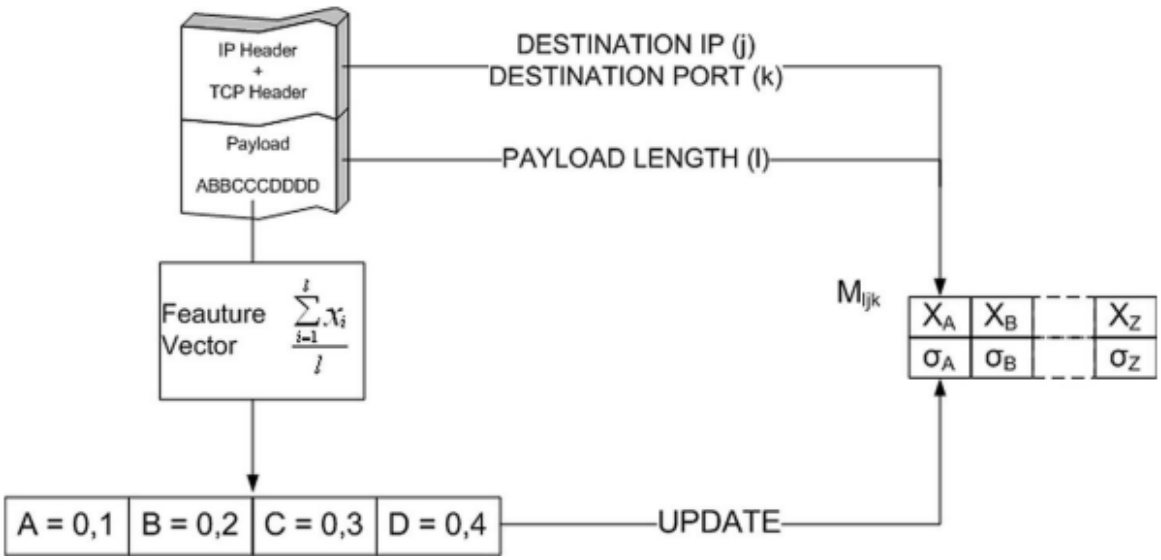
контрола на овој регистер напаѓачот ќе може да го искористи за извршување на програмски код којшто може да биде од малициозен карактер(backdoor).
Доколку овој тип на пропуст е од системски тип, тој може да предизвика DoS(denial of service) кој може да резултира со прекинување на работата на некој сервис.

Одредени типови на пропусти:
■ Red Hat lprd overflow
■ Linux samba overflow
■ IMAP login overflow
■ Linux mountd overflow

5 Алогоритми кои што се користат во IDS.

Како пример за алгоритми на IDS ќе ги претставиме PAYL и POSEIDON кои се дел од мрежните системи за неовластена детекција(NIDS) т.е аномалиски базирани системи. Аномалиски базираните NIDS можат во зависност од алгоритмите детекцијата да биде според заглавието на пакетите(packet headers), самото товариште/содржина(payload) што паќетот ја содржи или комбинација на двете. Payload базираните NIDS денес најчесто се користат за детекција на пакети кој имаат за цел да ги искористат софтверските пропусти на одреден компјутер од мрежата, па според тоа можеме да заклучиме дека тие се апликациски базирани.

5.1 PAYL (Wang and Stolfo) алгоритам.



Слика 3

На сликата 3 ни е прикажано архитектурата на PAYL алгоритмот којшто работи на следниов начин: најпрвин пакетите се подредени според полжината на товариштето(payload), а потоа се врши анализа на составните делови(n-gram) на самото товариште.

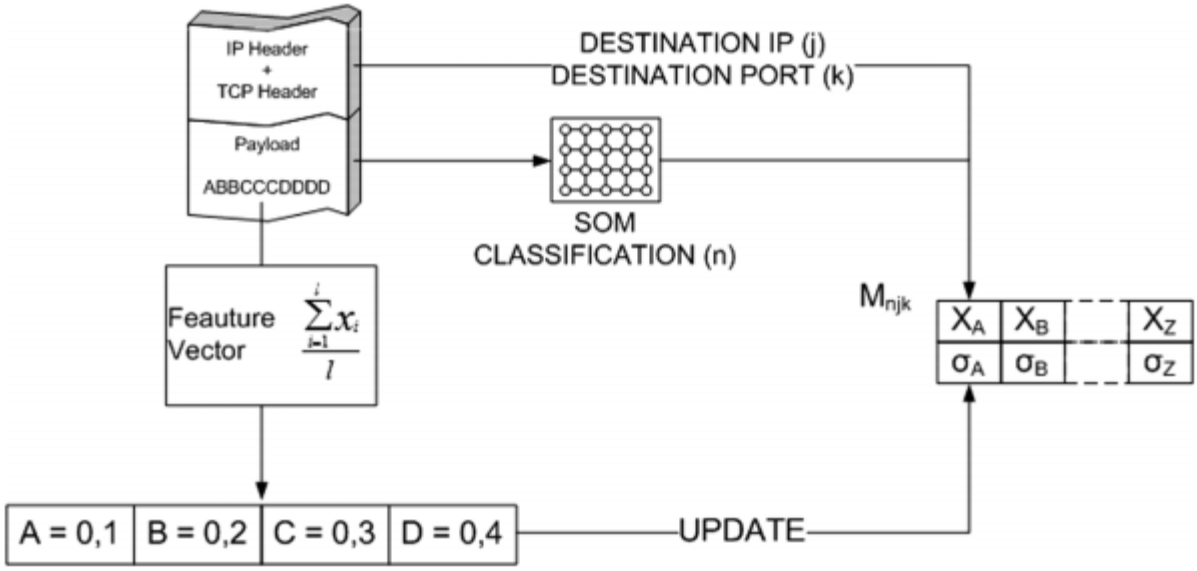
```
INPUT:
ip : IP адреса ∈ N
sp : порт ∈ N
l : должина на payload
x : PAYLOAD
Излез:
isAnomalous : BOOLEAN
/* Дали пакетот е аномален? */
dist := +∞
isAnomalous := FALSE
for each m ∈ M do
if (m.ip = ip and m.sp = sp and
m.l = l) then
dist := m.fv.getDistance(x)
/* get the distance between input */
/* data and associated model */
end if
done(for)
if (dist ≥ threshold) then
isAnomalous := TRUE
end if
return isAnomalous
```

Во тестирачката фаза, ќе ги земеме вредностите на должината, дестинациската IP адреса и TCP портот под одредени подмножества кои ќе ги обележеме со Tljk. Алгоритмот PAYL креира статистички модел на Tljk кадешто најпрвин прави анализа на составните делови(n-gram) на секој пакет од Tljk, и тогаш за секој составен дел се зачувува инкрементирачка вредност во еден вкупен статистички модел Mljk којшто исто така вклучува и вектор со среден број на бајти заеднички за сите фреквенции. Во текот на детектирачката фаза, истите вредности се добиваат од паќетите кои потоа се споредени со вредностите на моделот, во зависност од тоа дали има голема разлика на овие вредности со зададените вредностите зададени од корисникот се создава настан или тревога.

5.2 POSEIDON Алгоритам

Дизајнот на Poseidon беше со цел да се направи добар алгоритам без користење на метод на надзор на мрежните пакети. Ове е типичен проблем којшто можеме да го решеме со користење на невронски мрежи и особено со Self-Organizing Maps (SOM). SOM мапите глобално беа употребувани претходните години за калсицифирање на мрежните податоци со цел да се класифицираат и со цел да се детектираат одредени аномалии. Во POSEIDON, тие се употребени

за препроцесирање. Архитектурата на POSEIDON алогоритмот е всушност комбинација на SOM мапи со модифициран PAYL алгоритам и тој работи на следниов начин.



Слика 4

SOM мапата е употребена за препроцесирање на секој пакет, потоа PAYL алгоритмот прави класификација на вредност која ја добива од страна SOM мапата, за разлика од обичниот PAYL алгоритам кој ја користеше должината. Претходно PAYL користеше вкупен статички модел Mljk, но сега за разлика параметрите кои што ќе се користат место дестинацискатa адреса, сега ќе се користи дестинациска адреса и порт којшто ќе бидат на местото на променливата n.

Заклучок

Поради тоа што безбедноста е една од важните области во информатика, системите за детекција на неовластен пристап зафаќаат голема област од форензика, оперативни системи, компјутерска безбедност и програмирањето. Се запознавме со топологиите на архитектура коишто можат да бидат направени користејќи различни типови на IDS. Како главна карактеристика и основна цел на овие системи е детекција на малициозен напад којшто се состои од добивање на текот на извршување на програмите на еден систем т.е освојување на EIP регистерот т.е инструкцискиот покажувач кој ќе му овозможи извршување на малициозни код кој е составен од машински јазик (асемблер). Детекција на IDS се состои од детекција на пакетите кои содржат информации од малициозен карактер т.е инструкции познати како opcode (операциски кодови), којашто детекција се базира на дефинирани правила од страна на експерти.

Библиографија

1. http://ptgmedia.pearsoncmg.com/imprint_downloads/informit/perens/0131407333.pdf
2. http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
3. http://events.ccc.de/congress/2005/fahrplan/attachments/638-22c3_ids.pdf
4. http://www.networkintegritysystems.com/pdf/NIS-FiberOpticIntrusionDetectionSystems.pdf
5. http://www.cs.ucsb.edu/~seclab/projects/sploit/dbalzarotti_thesis.pdf
6. http://www.peterszor.com/blended.pdf