



МОНГОЛ УЛСЫН БОЛОВСРОЛЫН ИХ СУРГУУЛЬ
МАТЕМАТИК, БАЙГАЛИЙН УХААНЫ СУРГУУЛЬ

МЭДЭЭЛЭЛ ЗҮЙН ТЭНХИМ

Хонгорбаатар ХОНГОРЦЭЦЭГ

СҮЛЖЭЭНИЙ ХАЛДЛАГА ИЛРҮҮЛЭХ, ХАЛДЛАГААС СЭРГИЙЛЭХ
СИСТЕМИЙН СУДАЛГАА

D011401

БАКАЛАВРЫН ДИПЛОМЫН АЖИЛ

УЛААНБААТАР ХОТ
2020 ОН



МОНГОЛ УЛСЫН БОЛОВСРОЛЫН ИХ СУРГУУЛЬ
МАТЕМАТИК, БАЙГАЛИЙН УХААНЫ СУРГУУЛЬ

МЭДЭЭЛЭЛ ЗҮЙН ТЭНХИМ

Хонгорбаатар ХОНГОРЦЭЦЭГ

СҮЛЖЭЭНИЙ ХАЛДЛАГА ИЛРҮҮЛЭХ, ХАЛДЛАГААС СЭРГИЙЛЭХ
СИСТЕМИЙН СУДАЛГАА

D011401

БАКАЛАВРЫН ДИПЛОМЫН АЖИЛ

УДИРДАГЧ:

/Ц.НЯМСҮРЭН/

ШҮҮМЖЛЭГЧ:

/Т.БАТБОЛД /

УЛААНБААТАР ХОТ
2020 ОН

ГАРЧИГ

БҮЛЭГ 1. ОНОЛЫН СУДАЛГАА.....	3
1.1. Сүлжээний халдлага түүний төрөл.....	3
1.1.1. Автомат халдлага.....	3
1.1.2. Хүнээр удирдуулсан халдлага	4
1.2. Халдлага илрүүлэх систем	5
1.2.1. Хостод суурилсан халдлага илрүүлэх систем (HIDS)	5
1.2.2. Сүлжээнд суурилсан халдлага илрүүлэх систем (NIDS).....	6
1.2.3. Төвлөрсөн удирдлагатай халдлага илрүүлэх систем (DIDS).....	6
1.3. Халдлага эсэргүүцэх систем	6
1.4. Халдлага илрүүлэх, халдлагаас сэргийлэх системүүд.....	7
Дүгнэлт.....	9
БҮЛЭГ 2. ТУРШИЛТ СУДАЛГАА.....	10
2.1. SNORT халдлага илрүүлэх, эсэргүүцэх систем	10
2.2. SNORT халдлага илрүүлэх системийн үйл ажиллагааны зарчим.....	11
2.2.1. SNORT халдлага илрүүлэх системийн дүрмийн синтекс.....	12
2.3. SNORT халдлага илрүүлэх системийг суулгах.....	14
2.3.1. SNORT халдлага илрүүлэх системийг тохируулах.....	15
2.3.2. SNORT халдлага илрүүлэх систем дээр дүрэм нэмэх.....	15
2.3.3. Deamon хэлбэрээр ажиллуулах тохиргоо	16
2.3.4. Өгөгдлийн санд холбох тохиргоо.....	17
2.3.5. Вэб интерфейстэй холбох.....	18
2.4 SNORT-ийг турших.....	22
2.5 SNORT халдлага илрүүлэх системийг байрлуулах.....	23
2.6. DoS халдлага зогсоож байгаа эсэхийг шалгах туршилт	24
2.7. Snort системийн гарын авлага	25
НОМ ЗҮЙ.....	27

УДИРТГАЛ

Мэдээллийн эрин зуун болсон өнөө үед, дэлхий нийтээрээ даяарчлал, хувьсгал, шинэчлэл өөрчлөлтийг ар араасаа хурдацтай хийсээр байна. Мэдээллийн технологи асар хурдтайгаар хөгжиж, хийсвэр оюун ухаан, робот, IT, сүлжээ зэрэг нь салбартаа тэргүүлсээр, улам боловсронгуй хөгжиж бидний зайлшгүй мэдэх ёстой боловсрол болсон байна.

Харилцаа холбооны хэрэгсэл аль ч цаг үед эн тэргүүнд байсан тэгвэл гар утас нь улам боловсронгуй болсоор виртуал орчинд хүртэл холбоо барьж түүнчлэн, дүрс бичлэг, дуу зэрэг төрөл бүрийн үйл ажиллагаа хийдэг. Яаж холбоо барих бэ? та сүлжээний асуудлаа шийдчихсэн байхад л хангалттай. Та гар утсандаа хамгаалалт хийж нууц үг оруулдаг шиг, сүлжээнд ч бас нууц үг хамгаалалт хийх хэрэгтэй. Сүлжээний халдлага газар авч хэрэгтэй мэдээллээ хэрхэн хадгалах талаар асуулт тулгарна. Сүлжээний халдлагын хамгийн том илрүүлэлт бол халдлага илрүүлэх систем юм.

Энэхүү ажлын хүрээнд сүлжээний халдлага болон, сүлжээний халдлага илрүүлэх системүүдээс нээлттэй нэг системийг сонгон авч судалсан.

Сэдэв сонгосон үндэслэл

Хэт боловсонгүй хөгжлийн хурдыг дагаад сүлжээний халдлагын тоо ихэссэн. (Eyal Gruner, Нетанел Амар, 2015) Дэлхий дахинд цахим аюулгүй байдлаараа тэргүүлэгч компани “Nortonlifelock” өндөр хөгжилтэй 10 орны иргэдийн дунд судалгаа явуулахад 2019 онд нийт 499.2 сая хэрэглэгч цахим халдлагад өртсөн гэсэн дүн гарсан бөгөөд энэ нь өмнөх оноос 30 хувиар өссөн үзүүлэлт болжээ. (Л.Мөнхбат, 2007) [2]

Сүлжээний халдлага жил ирэх бүр улам түвэгтэй болсноор, хамгаалах арга зам, илрүүлэх систем болон мэдээллийн системийг хамгаалах арга хэрэгсэл ар араасаа боловсронгуй хөгжин гарсаар байна. Халдлагын маш олон төрлийн эрсдэлүүд байдаг тэдгээрийн зарим нь маш аюул хөнөөлтэй учир нь таны компьютерийн системийг бүхэлд нь устгаж болно. Төрөл бүрийн сүлжээний халдлагыг таних, халдлага илрүүлэх системийг хэрэглэх явдал нь асуудал шийдвэрлэх гарц гэвч өртөг өндөртэй байдаг учир халдлага илрүүлэх системийг тэр бүр худалдан авч чаддаггүй. Иймд сүлжээний халдлагын төрлүүдийг судалж, халдлагыг илрүүлэх нээлттэй нэг системийг сонгон авч судлахыг зорилоо.

Зорилго

Сүлжээний халдлага, түүний төрлийг судлах, халдлагаас сэргийлэх болон халдлага илрүүлэх системийн талаар судлах

Зорилт

- Сүлжээний халдлагын талаар үндсэн ойлголттой болох
- Сүлжээний халдлагын төрлүүдийг мэдэх
- Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх систем болох Snort програмыг судлах

БҮЛЭГ 1. ОНОЛЫН СУДАЛГАА

1.1. Сүлжээний халдлага түүний төрөл

Сүлжээний аюулгүй байдал нь сүлжээний халдлага, дайралт, зөвшөөрөлгүй хандахаас хамгаалж, сүлжээнд аюулгүй үйл ажиллагааг явуулахыг хэлдэг бол сүлжээнд санаатайгаар болон санамсаргүйгээр халдахыг халдлага гэнэ. Халдлагыг ерөнхийд нь дараах хоёр төрөлд ангилдаг.

1.1.1. Автомат халдлага

Энэ халдлага нь (viruses, Worms болон SQL Slammer г.м) идэвхтэй үйл ажиллагаа явуулдаг бөгөөд системд сөрөг нөлөө үзүүлдэг. Халдлага илрүүлэх системийг ашиглан тодорхой түвшинд эдгээр програмуудыг илрүүлэх боломжтой.

Virus программын аль нэг кодоод хавсрагдаж зөөгдөж, ачаалагдах замаар хөнөөлтэй үйл ажиллагаа явуулдаг.

Worm өөрөө бие даан сүлжээгээр тарж хөнөөлтэй үйл ажиллагаа явуулдаг. Өөрийгөө хувилж системд сөрөг нөлөөтэй үйлдлүүдийг хийдэг. Вирус болон worm-ийн дэвшилтэт хувилбар нь polymorphic буюу илрүүлэх програмаас зайлсхийхийн тулд шинж чанараа өөрчилж улам боловсронгуй болсон. Worm-ийн жишээ гэвэл 2003 оны нэгдүгээр сарын 25-нд илэрсэн SQLSlammer worm юм. Уг worm нь Microsoft Structured Query Language (SQL) серверийн сул талыг ашиглан хөнөөлтэй үйл ажиллагаа явуулдаг. SQL серверийн 1434 портоор 376 байтын User Datagram Protocol (UDP) протокол ашиглан дамжуулсан пакет нь buffer overflow халдлага хийдэг. Worm нь ойролцоогоор 10 минутад дэлхийгээр тархах боломжтой. Маш олон серверүүд worm-ийн халдлагад унаж байсан. Тухайлбал дэлхийн 13 үндсэн Domain Name Server-ийн 5 нь worm-ийн халдлагад унаж байсан¹. [3]

Автомат халдлагын жишээ: SQL Slammer/Sapphire халдлага

SQL Slammer/Sapphire 2003 оны 1 сарын сүүлээр шинээр Web Server вирус нь интернетээр тархсан бөгөөд энэхүү дайралтад маш олон компьютерийн сүлжээ бэлтгэлгүй байсны улмаас үйл ажиллагаа нь саатаж, хэд хэдэн чухал системийг тухайн вирус нь гацааж ажиллагаагүй болгосон байна. Америкийн АТМ-ийн

¹ <https://www.caak.mn/>

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа банкны үйлчилгээ доголдож, Seattle хот 911 үйлчилгээг авах боломжгүй болж, Continental Airline нь интернет захилга авах боломжгүйгээс болон хэд хэдэн нислэгээ цуцалж байсан юм. Энэхүү вирусийг мөн Sapphire гэдэг нэрээр нь хүмүүс мэддэг. Тооцоогоор, вирусийн эсрэг програм нь асуудлыг шийдэхээс өмнө тухайн вирус нь 1 тэрбум гаруй долларын хохирол учруулсан гэдэг. Slammer-ын довтолгооны тактик нь маш сайн зохион байгуулалттай байсан бөгөөд вирус нь анхны интернет сервертээ халдсаны дараа Slammer вирус нь хэдхэн секундийн дотор өөрийн тоогоо хоёр дахин хувилж, хурдтай тархаж байлаа. Анхны довтолгооноос 15 минутын дараа, Slammer вирус нь интернетийн тулгуур болсон серверүүдийн бараг талд нь халдсан байсан юм. Slammer вирусийн заасан үнэт хичээл нь: танд хамгийн сүүлийн үеийн вирусийн эсрэг програм болоод хамгаалалт байсан ч зарим тохиолдолд хангалтгүй байдаг. Хакерууд нь ямагт сул дорой цэг болоод олонд мэдэгдээгүй тэр л эмзэг газрыг нь хайж явдаг учраас вирус халдахаас өмнө ямар ч тохиолдолд гэсэн, хамгийн муу үйл явдалд бэлтгэлтэй байх нь чухал юм.

1.1.2. Хүнээр удирдуулсан халдлага

Тодорхой хугацаанд халдлагыг удирдах замаар хийж гүйцэтгэдэг. Халдлагыг хүн шууд удирдаж хийж гүйцэтгэх нь тухайн нөхцөлд таарсан оновчтой халдлага болох магадлалтай байдаг. Ийм төрлийн халдлагын жишээ бол Wingate POP3 buffer overflow халдлага юм. Уг халдлага нь POP3 дэймоний сул талыг ашиглан буфер дүүргэх буюу хэрэглэгчийн командыг илгээж ажиллуулах оролдлогыг хийдэг.

Хүнээр удирдуулсан халдлагын жишээ: Dos халдлага

DoS халдлага нь хоорондоо холбогдсон янз бүрийн компьютерүүд болон сүлжээнүүдийн хоорондох мэдээлэл, хялбар солигдохоор бүтээсэн программ ба 1973 оноос хойш их өдийг хүртэл дэлгэрэнгүй хөгжсөөр, серверт хамгийн их тохиолдсон халдлага юм. Сервер болон вэбэд их хэмжээний хүсэлт хандалт ирснээр вэб сервер уналтад орохыг DoS халдлага гэнэ.

DoS халдлага нь вэб серверийг тодорхой хугацаанд зогсоох, интернетэд холбогдсон компьютерийн үйлчилгээг зогсоох, сүлжээний нөөц байхгүй болгох зэрэг вэб сервер болон пакетын халдлага юм.

DoS халдлага нь түр буюу тодорхой бус хугацаагаар зогсоох юм уу эсвэл интернетэд холбогдсон компьютерийн үйлчилгээг зогсоох гэх мэт өөрийн зорилтот хэрэглэгчдэд нь сүлжээний нөөц байхгүй болгох гэсэн оролдлого юм. DoS-ийг

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа ихэвчлэн банк, кредит картын төлбөр зэрэг хувийн мэдээллийг үзэх мөн вэб сервер дээр зохион байгуулсан сайт эсвэл үйлчилгээг бууруулах зорилгоор DoS-ийг хийдэг². (wikipedia хөгжүүлэгч, 2016) [4]

DoS халдлагын төрлүүд:

- Peer-to-peer
- Teardrop
- Application level floods
- DDoS(Distributed Denial of Services)
- Nuke
- Reflected attack
- Unintentional attack
- Incident

DoS халдлагад өртөхөд интернэт удаан болох, вэб сервер идэвхгүй болох, вэб сайтруу орж болохгүй, хувийн мэдээллийг үзэх үед тодорхой хугацааны турш гацах зэрэг шинж тэмдэг илэрдэг.

1.2. Халдлага илрүүлэх систем

Халдлага илрүүлэх систем нь хортой үйл ажиллагаа, сүлжээнд хор учруулах, зөрчлийг хянах, тайлан болон өөр өөр замаар сэжигтэй урсгалыг илрүүлдэг.

Халдлага илрүүлэх, урьдчилан сэргийлэх систем (IDPS) халдлагыг танин мэдэх, тэдний тухай мэдээллийг нэвтрэн орж, халдлагын дайралтын тайлан эсэргүүцэхэд чиглэсэн байна. Үүнээс гадна, байгууллагууд, аюулгүй байдлын бодлогын асуудлыг тодорхойлж байгаа аюул заналыг баримтжуулах, аюулгүй байдлын бодлогыг зөрчсөн нь хувь тогтоон барих зэрэг бусад зорилгоор хувьд IDPSes ашигладаг. IDPSes бараг бүх байгууллагын аюулгүй байдлын дэд бүтцийг нь шаардлагатай нэмэлт болж байна. Халдлага илрүүлэх систем нь сүлжээнд учрах халдлагыг эсвэл ямар нэг хостод учрах халдлагыг шинжилж байгаа болон сүлжээнд тарсан байдлаар нь гурван төрөл болгон ангилж болно.^[3]

1.2.1. Хостод суурилсан халдлага илрүүлэх систем (HIDS)

Хостод суурилсан халдлага илрүүлэх систем нь дотоод сүлжээн дэх тухайн нэг компьютерийг хянах замаар хэрэгждэг. Халдлага илрүүлэх болон шалгахдаа системийн үйл ажиллагааг лог файлаас халдлагыг хайдаг. Дүрмийн бус үйл

² <https://mn.wikipedia.org/>

³ <https://mn.wikipedia.org/>

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа ажиллагаа болон зөвшөөрөлгүй хандалт, зэрэг нь лог файлаас илэрвэл дохиоллын системийг идэвхжүүлж систем халдлагад өртөж байгааг илрүүлнэ.

1.2.2. Сүлжээнд суурилсан халдлага илрүүлэх систем (NIDS)

Сүлжээнд суурилсан халдлага илрүүлэх систем нь сүлжээний рүү тэр эсвэл хостын түвшний пакетуудын мэдээлэлд анализ болон бүртгэл хийх замаар сэжигтэй пакетуудыг илрүүлж, дэлгэрэнгүй мэдээллийг лог файл руу бичдэг. Энэ төрлийн халдлага илрүүлэх систем нь халдлага илэрвэл системийн аюулгүй байдлын багийн гишүүдэд сануулгыг мэйлээр илгээнэ.

1.2.3. Төвлөрсөн удирдлагатай халдлага илрүүлэх систем (DIDS)

Төвлөрсөн удирдлагатай халдлага илрүүлэх систем нь сүлжээнд тархсан байдлаар суулгагдаж нэг төв нэгжид халдлагын тухай мэдээллийг цуглуулж төв өгөгдлийн санд хадгалдаг системийн төвлөрсөн удирдлагатай халдлага илрүүлэх систем гэнэ. Сүлжээний бүх хэсэгт халдлага илрүүлэх системүүд тархаж суулгагдсанаар зөвхөн төв шугамаар урсах traffic болон төв шугамаар дамжигдахгүй traffic-уудад шинжилгээ хийх боломжтой болохоос гадна сүлжээний хэсгүүдэд шинжилгээ хийсэн мэдээллийг нэг дор цуглуулах боломжтой болно. Сүлжээний администратор нэг дороос сүлжээг хянахад хялбар болдог.

Халдлага илрүүлэх систем нь ямар зам, ямар урсгалаар ирж байгааг тодорхойлон хамгаалах арга хэмжээ авна.

1.3. Халдлага эсэргүүцэх систем

Халдлага илрүүлэх системийг таслан зогсоох, дэд програмуудаар өргөтгөсөн системийг халдлага эсэргүүцэх систем гэнэ. Халдлага эсэргүүцэх системийг хаана байрлаж байгаагаар нь халдлага илрүүлэх системтэй адил гурав ангилж болно.

- ✓ Хостод суурилсан халдлага эсэргүүцэх систем (HIPS)
- ✓ Сүлжээнд суурилсан халдлага эсэргүүцэх систем (NIPS)
- ✓ Төвлөрсөн удирдлагатай халдлага эсэргүүцэх систем (DIPS)

Халдлага эсэргүүцэх системийг сонгохдоо сүлжээний гүйцэтгэл, нээлттэй эх, үйлдлийн систем, хөгжүүлэлт зэргийн нийцлийг харьцуулан харах хэрэгтэй. Халдлага эсэргүүцэх системийн халдлагыг таслан зогсоох дэд програмууд нь уг үр дүнд харгалзах үйлдлийг гүйцэтгэдэг.

Халдлага Эсэргүүцэх системд дараах шаардлагууд тавигдана. Үүнд:

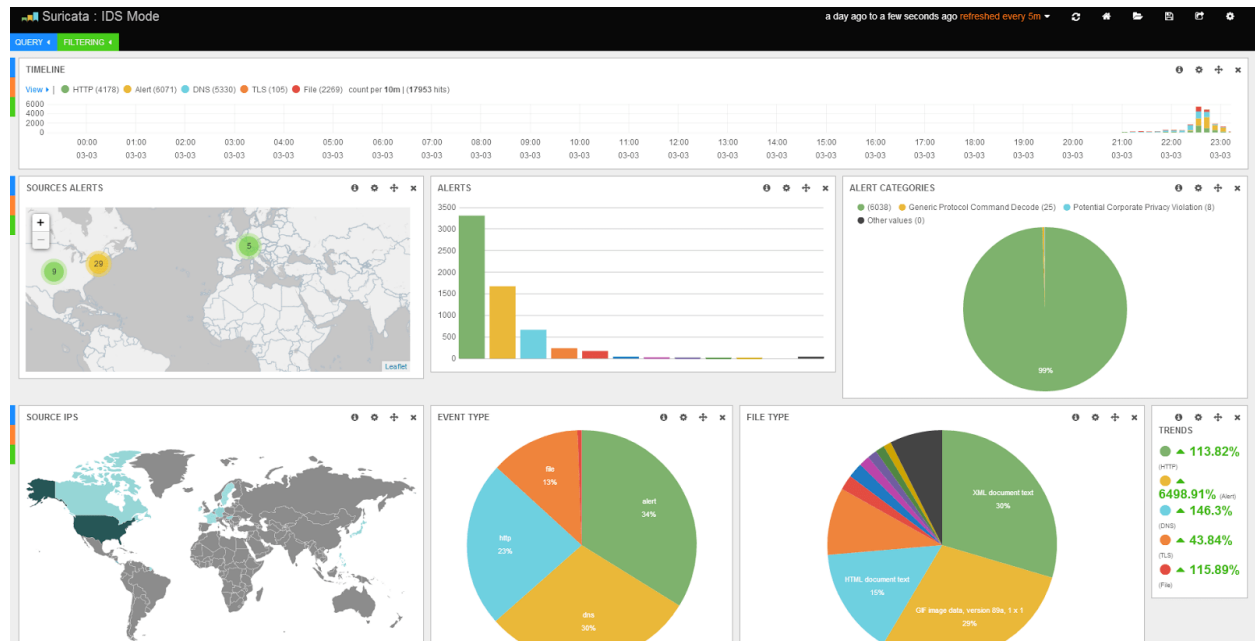
- Сүлжээний гүйцэтгэлийг удаашруулахгүй байх. Гарц дээр зөвхөн байрлаж сүлжээгээр дамжих ачааллыг нарийвчлан шинжилсний дараа л дамжуулдаг бол тухайн сүлжээний гарц дээрх хурдыг багасгана.
- Нээлттэй эх бүхий програм хангамж байх. Энэ нь халдлага эсэргүүцэх системийг маш бага зардлаар ашиглах боломж олгоно. Өөрөөр хэлбэл халдлага эсэргүүцэх системийг худалдаж авах зардал гаргахгүй байх боломж бүрдэнэ.
- Нээлттэй эх бүхий үйлдлийн системүүдийг дэмждэг байх. Энэ нь систем администратор тухайн сүлжээг нэг дороос хянахад маш хялбар болгох сайн шийдэл юм.
- Хөгжүүлэлт сайн хийгддэг байх. Хөгжүүлэлт сайн хийгддэг байх нь тухайн халдлага эсэргүүцэх системийг сайн гэж бүрэн дүүрэн нотлохгүй ч гэсэн нэлээд нөлөөтэй хүчин зүйл мөн. Учир нь халдлага хийх арга технологиуд маш хурдацтай хөгжиж байгаа учир түүнээс хамгаалах технологи нь мөн хурдан хөгжих шаардлагатай болж байгаа юм.

1.4. Халдлага илрүүлэх, халдлагаас сэргийлэх системүүд

Халдлага илрүүлэх, халдлагаас сэргийлэх хоёр систем нэгэн зэрэг ажилладаг хэд хэдэн нээлттэй эхийн хэрэгслүүд байдаг. Эдгээрээс хамгийн сайн бөгөөд өргөн хэрэглэгддэг 5 хэрэгслийн талаар судалж, мэдээллийг орууллаа.

1. **Snort** - Windows болон Unix үйлдлийн системд ашиглаж болдог бодит хугацаанд өгөгдөлд анализ хийж халдлагыг илрүүлэх, халдлагаас сэргийлэх боломжтой. Үндсэн Snort програм нь үнэгүй, чөлөөтэй ашиглаж болохоор байдаг. Snort-ийн худалдааны хувилбарыг SourceFile програм үйлдвэрлэдэг бөгөөд 2013 онд Cisco компанийн худалдан авснаар Cisco-гийн аюулгүй байдлын хамгаалалтын бүтээгдэхүүнүүд Snort-ийн нээлттэй эхийн технологийг дэмжих болсон. Сул тал нь хэрэглэгчийн интерфэйс байхгүй гэвч хэрэглэгчдийн хөгжүүлсэн add-ons нэмж болдог. Пакет шалгах нь удаан байдаг.
2. **Suricata** – Snort-той төстэй, сүлжээн дэх халдлагаас сэргийлэх, халдлага илрүүлэх, сүлжээний аюулгүй байдлыг хянах боломжтой хэрэгсэл. Ашгийн бус нийгэмлэг OISF нь энэхүү хэрэгслийн нээлттэй эхийг эзэмшиж, хөгжүүлж

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа байдаг. Түүний дэмжин ажилладаг үйлдвэрлэгчид нь FireEye, Proofpoint, Positive Technology зэрэг болно. Сул тал нь буруу мэдээлэл гаргах тал байдаг. Зурагт Suricata програмын хяналтын дэлгэцийг харуулав.



Зураг 1. Suricata програмын хяналтын дэлгэц

- OSSEC** - Олон үйлдлийн системд ашиглаж болох хостод суурилсан халдлага илрүүлэх, халдлагаас сэргийлэх хэрэгсэл юм. Анализ хийх хүчирхэг хэрэгсэлтэй, файл шалгах, лог шалгах, бодит хугацааны мэдэгдэл гаргах зэрэг олон үйлдэлтэй байдаг. Зурагт Unix үйлдлийн системд ажиллаж буй системийн дэлгэцийг харуулав.
- Security Onion** – Linux үйлдлийн системд зөвхөн ажиллах зориулалттай сүлжээний аюулгүй байдлыг хянах, лог удирдах, халдлага илрүүлэх боломжтой нээлттэй систем.
- Zeek - Bro Network Security Monitor** – Bro нь сүлжээний аюулгүй байдлын нээлттэй систем. Berkeley дахь олон улсын компьютерийн шинжлэх ухааны институт болон Urbana-Champaign-ий Supercomputing Applications үндэсний төвийн судлаачдын хөгжүүлдэг нээлттэй систем. Сүлжээний траффикт анализ хийх түүний аюулгүй байдлыг хянах, халдлага илрүүлэх, лог бичих зориулалттайгаар гарсан байна. Сул тал нь програмчлалын мэдлэг, туршлага шаарддаг.

Дүгнэлт

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системүүдийг судалсны үндсэн дээр дэлхийд хамгийн өргөн хэрэглэгддэг систем болох Snort-ийг дэлгэрэнгүй судлахаар сонгон авав.

Энэхүү системийн үнэгүй хувилбарыг одоогийн байдлаар 4 сая хүн татан авсан үзүүлэлт байгаа нь энэ төрлийн системүүд дотроо хамгийн эрэлт, хэрэгцээтэй байгааг нь илтгэж байгаа юм.

Мөн 2020 оны хамгийн шилдэг халдлага илрүүлэх, халдлагаас сэргийлэх нээлттэй эхийн системүүдийн 1-т жагсаж байна⁴.

⁴ <https://www.upguard.com/blog/top-free-network-based-intrusion-detection-systems-ids-for-the-enterprise>

БҮЛЭГ 2. ТУРШИЛТ СУДАЛГАА

2.1. SNORT халдлага илрүүлэх, эсэргүүцэх систем

Snort IPS нь хор хөнөөлтэй сүлжээний үйл ажиллагааг тодорхойлоход туслах хэд хэдэн дүрмийг ашигладаг бөгөөд тэдгээр дүрмүүдтэй тохирсон пакетуудыг хайж олоход хэрэглэгчдэд сэрэмжлүүлэг өгдөг.

Snort нь гурван үндсэн хэрэглээтэй: tcpdump шиг пакет үнэрлэгч, пакет бүртгэгч гэх мэт - сүлжээний траффик шалгахад тустай, эсвэл сүлжээний нэвтрэлтээс урьдчилан сэргийлэх систем болгон ашиглаж болно. Snort-ийг хувийн болон бизнесийн зорилгоор татаж авах, тохируулах боломжтой.

Snort нь IP сүлжээнд бодит хугацааны трафикийг шинжилгээ хийж пакетуудыг бүртгэдэг боломж бүхий сүлжээний халдлагыг илрүүлэх (NIDS) болон сүлжээний халдлагаас урьдчилан сэргийлэх (NIPS) нээлттэй эхийн үнэгүй систем юм.

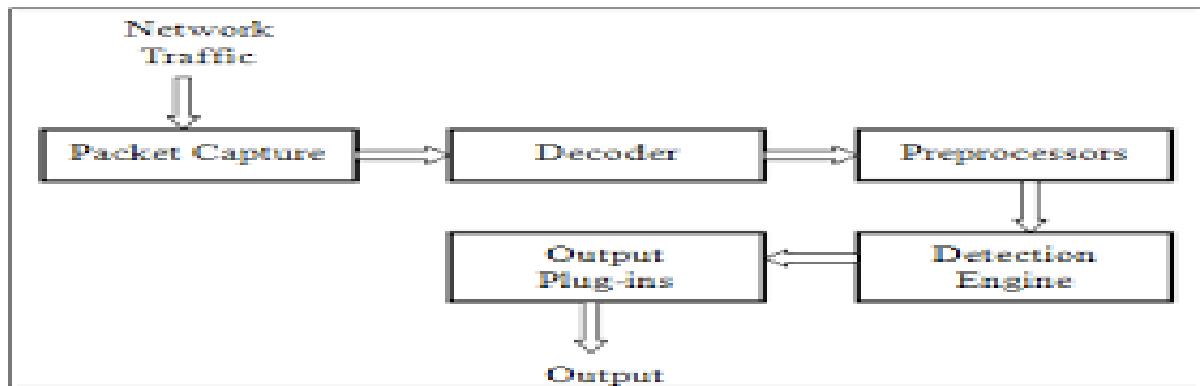
Snort нь протокол шинжилгээг хийж, агуулгаас хайлт хийхээс гадна OS fingerprint оролдлого, SMB судалгаа, вэб application довтолгоо, нэвтрэх боломжит порт шалгалтууд, буфер дүүргэлтийн алдаа шалгалт болон бусад халдлага, шинжлэгч нарыг пассив илрүүлэх, актив блоклоход ихэвчлэн хэрэглэгддэг хэрэгсэл юм⁵. (wikipedia хөгжүүлэгч нар, 2016) [5]

Unix төст системд libpcap буюу windows системд winpcap гэх сүлжээний траффикийг тодорхой форматтайгаар файлд хадгалдаг application programming interface ашиглан пакетуудыг барьдаг. Тухайлбал Snort нь packet sniffing горимд пакетыг уншиж байх үедээ pcap (Packet CAPture library)-ийг ашиглан Process Packet функцийг дуудаж ажиллуулан пакетыг бүтцээр нь задална. Дараа нь IDS горимд шилжин уг пакетыг шалгаж үнэлгээ дүгнэлт өгнө. Эцэст нь packet-лог горимд шилжин гаралтын plug-in-уудыг дуудаж ажиллуулах замаар alert-уудыг үүсгэдэг.

Ихэвчлэн бидний шалгахыг хүссэн пакетууд интернетээс ирдэг тул таны Snort мэдрэгч нь таны дотоод сүлжээг гадаад ертөнцөөс тусгаарлаж, периметр дээр байх болно. Мэдрэгчийг хаана байрлуулахыг хүсэж байна (жишээлбэл, галт хананы өмнө, дараа эсвэл дотор талд), энэ нь танаас хамаарна. Хэрэв та бүх

⁵ Wikipedia link

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа траффикийг харахыг хүсвэл дараах схемийг баримтална уу: Internet> Router> Sensor> Firewall> Switch> Дотоод сүлжээ. Нөгөө талаас, хэрэв та мэдрэгчийг галт хананы өмнө байрлуулахыг хүсэж байвал галт ханаар дамжин өнгөрөх хөдөлгөөнийг л харах боломжтой болно. Энэ тохиолдолд та Интернет> Чиглүүлэгч> Галт хана> Мэдрэгч> Шилжүүлэгч> Дотоод сүлжээ гэсэн схемийг дагаж мөрдөх болно. Snort мэдрэгчийг траффик хянахыг хүссэн газартаа байрлуулж болно..



Зураг 2. Snort халдлага илрүүлэх системийн үйл ажиллагааны зарчим. UMUC, 2012

Сүлжээний траффик нь "Пакет декодер" -оор дамжин өнгөрөх болно. Энэ нь PPP холболт, Ethernet (зэс эсвэл шилэн кабелийн) холболт юм. Пакет декодерын зорилго нь урьдчилан боловсруулагчдын багцыг бэлтгэх явдал юм.

"Урьдчилан боловсруулагч" нь урсгалыг хүлээн авдаг бөгөөд ингэснээр Snort урьдчилсан процессорын залгааснууд нь TCP урсгалыг дахин угсрах, IP defragmentation, статистик мэдээлэл цуглуулах эсвэл HTTP хүсэлтийг хэвийн болгох зэрэг маш нарийн түвэгтэй функцүүдийг гүйцэтгэх боломжийг олгодог. Та "spp_something.c" болон "spp_something.h" файлуудыг өөрчилж Snort preprocessor залгааснуудыг нэмж болно. Эцсийн үүрэг бол илрүүлэх хөдөлгүүрийн дүрмүүдтэй харьцуулахын тулд пакетуудыг өөрчлөх явдал юм. (Сэтгүүл , 2018) [6]

2.2. SNORT халдлага илрүүлэх системийн үйл ажиллагааны зарчим

Snort нь гарын үсэг дээр суурилсан NIDS / NIPS тул урьдчилан тогтоосон дүрмийг баримталдаг. Snort дүрмүүд нь хоёр хэсгээс бүрдэнэ. "Толгой" нь Snort-ийн хийх арга хэмжээг зааж өгнө. Үүнд дүрмийн үйл ажиллагааны талаарх бүртгэл, сэрэмжлүүлэх зэрэг хүчин зүйлс орно. Толгой хэсэгт Snort дүрмийн эх сурвалж, хүлээн авах болон илгээх IP хаяг, хүлээн авах портын дугаар, ашиглагдаж буй протокол зэргийг багтаасан хэсгийг агуулна. Snort дүрмийн хоёр дахь хэсэг нь

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа “Сонголтууд” юм. Сонголтууд бол аюулгүй байдлын пакетэд юу багтдаг, снорт дүрмийг пакеттай тааруулахад гарч ирэх мессежийг тодорхойлох боломжтой.

Хүснэгт 1. Снорт дүрмийн бүтэц

Толгой						Сонголтууд	
Дүрэм үйл ажиллагаа	Протокол	Илгээгч IP хаяг	Илгээгч порт	Урсгал чиглэл	Хүлээн авах IP хаяг	Хүлээн авах порт	Нэмэлт тест, гаралтын мессеж гэх мэт

2.2.1. SNORT халдлага илрүүлэх системийн дүрмийн синтекс

Snort нь орж ирсэн пакетыг хөнөөлтэй үйл ажиллагаа явуулах пакет мөн гэдгийг танихын тулд дүрэм ашигладаг. Дүрмүүдийг хэрхэн тохиромжтой бичсэнээс халдлага илрүүлэх систем нь халдлагыг оновчтой тодорхойлж мэдэгдэл гаргах нь хамаарна. Иймд дүрмүүдийг зөв сонгох нь чухал юм.

Дүрмийг өөрийн системд тохиромжтой байдлаар бичих шаардлагатай байдаг боловч Snort-ийг хөгжүүлдэг багаас зөвлөмж болгож өөрсдийнх нь гаргадаг дүрмүүдийг албан ёсны сайтдаа үнэгүй татах боломжтойгоор байрлуулсан байдаг.

Гэхдээ тухайн сайтад бүртгэгдээгүй хэрэглэгчид нэмэлт сайжруулалт хийгддэггүй дүрмүүдийг л татах боломжтой, бүртгэгдсэн хэрэглэгчид нь шинэ гарсан дүрмүүдийг 30 хоногийн дараанаас татах боломжтой болно, бүртгэгдээд төлбөр төлсөн хэрэглэгчид болон хөгжүүлэгчид нь шинэ дүрмийг гарсан дариуд нь авах боломжтой байдаг. Шинэ дүрэм гарахаараа бүртгэгдсэн хэрэглэгчдийн и-мэйл хаягаар нь мэдэгддэг.

Snort нь тодорхой синтаксийг дагаж мөрддөг. Энэ нь галт хананы дүрмүүдтэй төстэй боловч Options хэсэг нь галт хананаас илүү давуу тал болж өгдөг. Дүрмийн синтакс задаргааг нэг бүрчлэн доор тайлбарлав.

Дүрмийн үйл ажиллагаа: Энэ талбарт та бүртгэлийн, сэрэмжлүүлэх, дамжуулах, идэвхжүүлэх эсвэл динамик таван дүрмийн үйлдлүүдийн аль нэгийг нь сонгож болно. Хамгийн нийтлэг дүрмийн үйлдэл бол "сэрэмжлүүлэх" сонголт бөгөөд пакет болон хийсэн үйлдлийг бүртгэж дараа нь аюулгүй байдлын администраторт анхааруулга өгдөг.

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа

Протокол: Энэ нь HTTP гэх мэт өндөр түвшний протокол, TCP, UDP, ICMP зэрэг доод түвшний протокол гэх мэт ашиглагдаж буй протоколыг тодорхойлдог. Та өөрийн тодорхой дүрмийг бий болгохын тулд аль алиныг нь сонгож болно.

Илгээгчийн IP хаяг: Энэ талбар нь пакетийг илгээгчийн хаяг юм. Энэ нь ганц IP хаяг эсвэл сүлжээний ID байж болно. Жишээлбэл, та ямар нэгэн илгээгч IP хаягаас ирэх бүх урсгалыг анхааруулахыг хүсвэл "any" -г ашиглаж болно.

Илгээгчийн порт хаяг: Энэ талбар нь пакетийн эх TCP эсвэл UDP порт юм. Дахин хэлэхэд, хэрэв та бүх 65,535 портыг зааж өгөхийг хүсвэл "any" -ийг ашиглаж болно.

Урсгал (Чиглэл): Энэ талбар нь ихэвчлэн "->" (чиглэлтэй сум) тэмдгийг ашиглан пакет урсгалын чиглэлийг тодорхойлдог.

Хүлээн авах IP хаяг: Энэ бол пакет руу очих зориулалттай газар юм. Энэ нь ганц IP хаяг, сүлжээний ID эсвэл "дурын" хаяг байж болно.

Хүлээн авах Port хаяг: Энэ бол пакет руу очих зориулалттай TCP эсвэл UDP порт юм. Энэ нь ганц IP хаяг, сүлжээний ID эсвэл "дурын" хаяг байж болно.

Сонголтууд: Өмнө дурдсанчлан Snort-ийн гол ашиглах хэсэг Options хэсэгт байна. Snort дүрмийн сонголтууд нь дүрмийг өөрөө боловсронгуй болгоход тусалдаг.

Агуулга: Энэ бол пакет ачааны доторх мөрийн хэв маягийг олоход хэрэглэгддэг түлхүүр үг юм. Энэ нь ASCII, хоёртын эсвэл арван зургаатын форматтай байж болно. Жишээлбэл, хортой програмын зарим хэлбэр нь тодорхой хоёртын эсвэл арван зургаатын мөртэй байдаг. Хэрэв та энэ мөрийг мэддэг бол үүнийг энд зааж өгөх боломжтой бөгөөд хэрэв таны сүлжээнээс үүнийг олж мэдвэл Snort танд анхааруулах болно.

Оффсет: Оффсет түлхүүр үгийг пакет доторх тодорхой байтын дараа хайлтын эхлэлийг зааж өгөхөд ашиглаж болно. Жишээлбэл, хэрэв та пакет доторх тодорхой байтын дараа хайлтаа эхлүүлэхийг хүсвэл энд бичиж болно.

Гүн: Гүнзгий түлхүүр үг нь пакет доторх тодорхой байтаар хязгаарлагдах хайлтыг тодорхойлоход хэрэглэгддэг. Энэ нь Offset сонголттой төстэй;

Тохиолдол: Энэ нь хайлтын үед том, жижиг үсгийг ялгах эсэхийг тохируулах хэсэг юм.

Агуулгын жагсаалт: Энэ түлхүүр үг нь "нууц үг", "ssn" гэх мэт түлхүүр үг агуулсан тодорхой текст файлыг олоход хэрэглэгддэг. Жишээлбэл, Snort эдгээр түлхүүр үгсийн файлыг хайж олох боломжтой. Та Snort-г интернет хайлт хийхэд ашиглаж болно гэдэгт би итгэж байна. Жишээлбэл, хэрэв хэрэглэгч "порно" гэсэн түлхүүр үгийг хайж байсан бол аюулгүй байдлын администраторт анхааруулга өгөх болно.

Тугууд: тугуудын түлхүүр үгийг TCP толгой хэсэгт байрлуулсан алга болсон эсвэл тохиромжгүй тугуудыг илрүүлэхэд ашиглаж болно. Заримдаа алга болсон тугууд нь портыг сканнердах эсвэл дайрах шинж тэмдэг болдог. [6]

Snort дүрмүүд нь халдлага, хор хөнөөлтэй үйл ажиллагааг илрүүлдэг. Та сэрэмжлүүлэх, бүртгэл хийх, холболтыг таслах гэх мэт тодорхой дүрмүүдийг бичиж болно. Дүрмүүд нь энгийн синтакстай байдаг. Түүнчлэн, та бүх дүрмийг тохиргооны файлд бичиж, өөр системд тохирох зүйлээ засах боломжтой.

Snort нь гурван өөр горимтой. Эдгээр горимууд нь;

- Пакет Sniffer
- Пакет бүртгэгч
- NIPDS (Сүлжээнд нэвтрэх, урьдчилан сэргийлэх системийг илрүүлэх систем)

2.3. SNORT халдлага илрүүлэх системийг суулгах

Snort-ийг windows систем дээр суулгахдаа www.Snort.org татаж аваад step-to-step байдлаар суулгаж болно харин unix төст системүүд дээр эх кодыг нь татаж аваад компайл хийх, rpm багцыг нь татаж аваад суулгах боломжтой. Харин fedora project-д Snort-ийг fedora-д зориулан тохиргоо хийсэн кодыг бэлдсэн байдаг учир Snort-ийг fedora дээр yum install командаар суулгах боломжтой байдаг. Иймд Snort-ийг зөвхөн халдлага илрүүлэх систем байдлаар ажиллуулах тохиолдолд install командаар суулгах нь тохиромжтой. Snort-ийн бүх холбоотой багцуудыг суулгах бол “yum install Snort*” гэсэн командаар суулгаж болно. Харин зөвхөн mysql өгөгдлийн санд alert болон лог-уудаа хадгалдаг байхаар ашиглах бол yum install “Snort Snort-mysql” гэсэн командаар суулгах нь тохиромжтой. Ингэсэн тохиолдолд зөвхөн Snort нь mysql өгөгдлийн сантай холбогдох гаралтын plugin-тайгаа л сууна.

```
[root@localхост /]# yum install Snort*
```

```
Installed: Snort.i386 0:2.8.1-4.fc9 Snort-bloat.i386 0:2.8.1-4.fc9 Snort-mysql.i386
```

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа
0:2.8.1-4.fc9 Snort-mysql+flexresp.i386 0:2.8.1-4.fc9 Snort-plain+flexresp.i386 0:2.8.1-4.fc9 Snort-postgresql.i386 0:2.8.1-4.fc9 Snort-postgresql+flexresp.i386 0:2.8.1-4.fc9 Snort-snmp.i386 0:2.8.1-4.fc9 Snort-snmp+flexresp.i386 0:2.8.1-4.fc9

Dependency Installed: libprelude.i386 0:0.9.17.2-1.fc9 mysql-libs.i386 0:5.0.51a-1.fc9 postgresql-libs.i386 0:8.3.4-1.fc9

2.3.1. SNORT халдлага илрүүлэх системийг тохируулах

Халдлагыг зөв тодорхойлох болон хэрэгцээтэй мэдээллээ цуглуулах нь Snort-ийг хэр зэрэг тухайн системд тохирсон оновчтой тохируулга хийж чадсанаас хамаарна. Иймд Snort-ийг тохируулахдаа дүрэм сонгох, ямар горимд ажиллуулах, өгөгдлийн сан ашиглах эсэхийг оновчтой байдлаар сонгох шаардлагатай.

Snort-ийн үндсэн тохиргооны файл нь fedora-ийн хувьд /etc/Snort/Snort.conf файл байдаг. Энэ файл дотор дүрмүүдийг тодорхойлох, гадаад болон дотоод сүлжээг ялгах, өгөгдлийн сантай холбох, server-үүдийн хаягийг заах (тухайлбал dns query-ийг alert болгож гаргахгүйн тулд dns server ямар хаяган дээр байгааг тодорхойлдог) зэрэг үндсэн тохиргоог хийдэг.

2.3.2. SNORT халдлага илрүүлэх систем дээр дүрэм нэмэх

Snort нь орж ирсэн пакетыг хөнөөлтэй үйл ажиллагаа явуулах пакет гэдгийг танихын тулд дүрэм ашигладаг. Дүрмүүдийг хэрхэн тохиромжтой бичсэнээс халдлага илрүүлэх систем нь халдлагыг оновчтой тодорхойлж alert гаргах нь хамаарна. Иймд дүрмүүдийг зөв сонгох нь чухал байдаг.

Өөрийн тодорхойлсон болон татаж авсан дүрмүүдийг ашиглахын тулд Snort-ийн үндсэн тохиргооны файлд оруулах шаардлагатай. Өөрөөр хэлбэл Snort-ийн үндсэн тохиргооны файлд дүрмийг тодорхойлж байгаа бичлэгийг нэмэх эсвэл Snort-ийн албан ёсны сайтаас татаж авсан дүрмүүд байрлах замыг зааж өгч include командаар сонгосон дүрмүүдийг үндсэн тохиргооны файлд оруулах шаардлагатай. Анхны утгаараа Snort-ийн үндсэн тохиргооны файлд “var RULE_PATH/etc/Snort/rules” гэсэн байдлаар дүрмүүдийн байрлах замыг тодорхойлсон байдаг. Иймд татаж авсан дүрмүүдийг /etc/Snort/rules хавтсанд хуулаад үндсэн тохиргооны файл дээр include командаар оруулснаар тухайн дүрмийг ашиглах боломжтой болно.

Тухайлбал scan хийдэг дүрмийг татаж аваад /etc/Snort/rules хавтсанд хуулсан

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа
байлаа гэхэд /etc/Snort/Snort.conf файлд дараах бичлэгийг нэмэх ёстой.

```
include $Rule_PATH/scan.rule
```

2.3.3. Daemon хэлбэрээр ажиллуулах тохиргоо

Системийн администратор тухайн хугацаанд Snort-ийг команд ашиглан ажиллуулна гэдэг нь администратор командыг хийж ажиллуулж байгаа season- оо хаахад Snort мөн ажиллахгүй болох учир энэ нь тохиромжгүй үйлдэл бөгөөд daemon хэлбэрээр ажиллуулах нь тохиромжтой. Тухайлбал Snort суулгасан машин унтарч ассан ч ажилладаг байхаар тохируулах үед энэ тохиргоо нь хэрэглэгдэнэ.

/etc/init.d/Snort файл дотор Snort-ийг daemon хэлбэрээр ажиллахад шаардагдах тохиргоонуудыг хийнэ. Тухайлбал service-ийг ачаалахад Snort нь ямар option-той ажиллах вэ гэдгийг тохируулна. “-D” option нь daemon горимд ажиллана гэдгийн заана, “-u” ямар хэрэглэгчийн эрхээр ажиллана гэдгийг заана.

Тухайлбал /etc/init.d/Snortd файлыг доор үзүүлсэн байдлаар тохируулж болно.

```
case "$1" in start)
echo -n "Starting Snort: " cd /var/лог/Snort
daemon /usr/sbin/Snort -D $SNORT_OPTIONS -u $USER -g $GROUP \
-i $INTERFACE -c /etc/Snort/Snort.conf touch /var/lock/subsys/Snort
echo
;;
stop)
echo -n "Stopping Snort: " killproc Snort
rm -f /var/lock/subsys/Snort echo
;;
restart)
$0 stop
$0 start
;;
status)
status Snort
;;
*)
Echn "Usage: So {start|stop|restart|status}"exit 1
```

Esac

Exit 0

2.3.4. Өгөгдлийн санд холбох тохиргоо

Snort нь пакетыг барьж аваад хадгалах замаар их хэмжээний лог болон alert-ийг үүсгэдэг учир тэдгээрийг файлд хадгалсан байдлаар нь удирдан зохицуулах нь түвэгтэй байдаг энэ байдлыг шийдвэрлэхийн тулд өгөгдлийн сантай холбож тэдгээр лог болон alert-ийг ангилан хадгалдаг. Энэ ажилдаа Snort-ийг mysql-тэй холбож лог болон alert-уудыг нь өгөгдлийн санд хадгалдаг болгосон.

Ингэхийн тулд mysql-ийг суулгасан байх шаардлагатай. Хэрэв суулгаагүй бол fedora дээр yum install командаар суулгах боломжтой.

```
#yum install mysql mysql-server Installed: mysql-server.i386 0:5.0.51a-1.fc9 ,  
mysql- 5.0.51a-1.fc9.i386
```

Mysql-ийг суулгасны дараа mysql-ээ demon хэлбэрээр ажиллуулах

```
# service mysqld start
```

Mysql admin-ий нууц үгийг тохируулах

```
# mysqladmin -u root password [нууц үг]
```

Mysql рүү root хэрэглэгчийн эрхээр нэвтрэх # mysql -u root -p

Snort-д зориулан лог болон alert-ийг хадгалдаг өгөгдлийн сан үүсгэх

```
mysql> CREATE DATABASE Snort; Query OK, 1 row affected (0.12 sec)
```

Snort-ийн өгөгдлийн санд хандах хэрэглэгчийг үүсгэх болон тухайн хэрэглэгчийн тухайн өгөгдлийн санд хандах эрх болон нууц үгийг нь тодорхойлох

```
mysql> grant all privileges on Snort.* to Snortusr@"localхост" identified by 'нууц үг';
```

```
Query OK, 0 rows affected (0.00 sec)
```

Өмнө хийсэн командыг идэвхжүүлэх.

```
mysql> flush privileges; Query OK, 0 rows affected (0.00 sec)
```

Үүсгэсэн өгөгдлийн сандаа лог болон alert хадгалахад хэрэглэгдэх хүснэгтүүдийг нэмэх. Yum install командаар Snort-ийг суулгах үед /usr/share/doc/Snort-2.8.1/create_mysql файл хуулагдсан байдаг. Уг файл нь уг хүснэгтүүдийг өгөгдлийн санд дараах командаар оруулж болно.

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа
#mysql -u root -p < /usr/share/doc/Snort-2.8.1/create_mysql Snort

Snort-ийг өгөгдлийн сантай холбохдоо үндсэн тохиргооны файл дээр нь дараах бичлэгийг нэмнэ. Энэ бичлэг нь Snort-ийг өгөгдлийн сантайгаа холбогдоход нь хэрэглэгдэх тохиргоо бөгөөд өмнө нь суулгасан Snort-mysql plugin-ийг тохируулж байна гэсэн үг. Тухайлбал лог эсвэл alert-ийн алийг нь хадгалахыг заах, өгөгдлийн сангийн төрөл (mysql, mssql, postgresql-ийн аль нь гэдгийг), өгөгдлийн санд хандахад хэрэглэгдэх хэрэглэгчийн нэр болон нууц үг зэргийг тодорхойлсон байна. Тухайлбал дараах байдлаар бичиж оруулна. output database: лог, mysql, user=Snort password=нууц үг dbname=Snort хост=localhost

2.3.5. Вэб интерфэйстэй холбох

Snort-ийн command line интерфэйсийг хэрэглэх нь өргөн боломжтой байдаг боловч хэрэглэхэд түвэгтэй байдаг. Иймд вэб интерфэйс холбож өгөгдлийн санд хадгалагдсан лог болон alert-ууд дээр задлан шинжилгээ хийх боломжтой.

Snort-д холбох боломжтой base болон acid зэрэг вэб интерфэйс буюу php site-ууд байдаг. Энэ туршилтын ажлаараа би base-ийг суулгасан. Учир нь base нь acid-аас илүү хэрэглэх өргөн боломжтой байдаг. Тухайлбал acid нь alert-уудыг цагийн бүсээр нь ангилж үзүүлдэггүй.

Php хуудсуудыг ажиллуулахдаа apache болон php-ийг суулган ажиллуулж болно. Тэдгээрийг fedora дээр дараах байдлаар yum install командаар суулгаж болно.

```
#yum install httpd php php-mysql
```

Вэб интерфэйсийг холбохын тулд дараах php site-уудыг татаж авна.

- Base:

http://sourceforge.net/project/showfiles.php?group_id=103348&package_id=128846&release_id=617636

- ADODB: <http://phplens.com/lens/dl/adodb453.tgz>

Эдгээр нь adodb*.tgz болон base.tar.gz файлууд байх бөгөөд тэдгээрийг задлаад вэб сервер ажиллаж байгаа directory-т хуулна. Тухайлбал дараах командуудыг ашиглан хуулж болно.

```
$tar -xvzf ~/adodb453.tgz
$mv ~/adodb453 /var/www/html/adodb
$tar -xvf ~/base-1.4.1.tar.gz
$mv ~/base-php4 /var/www/html/base
```

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа

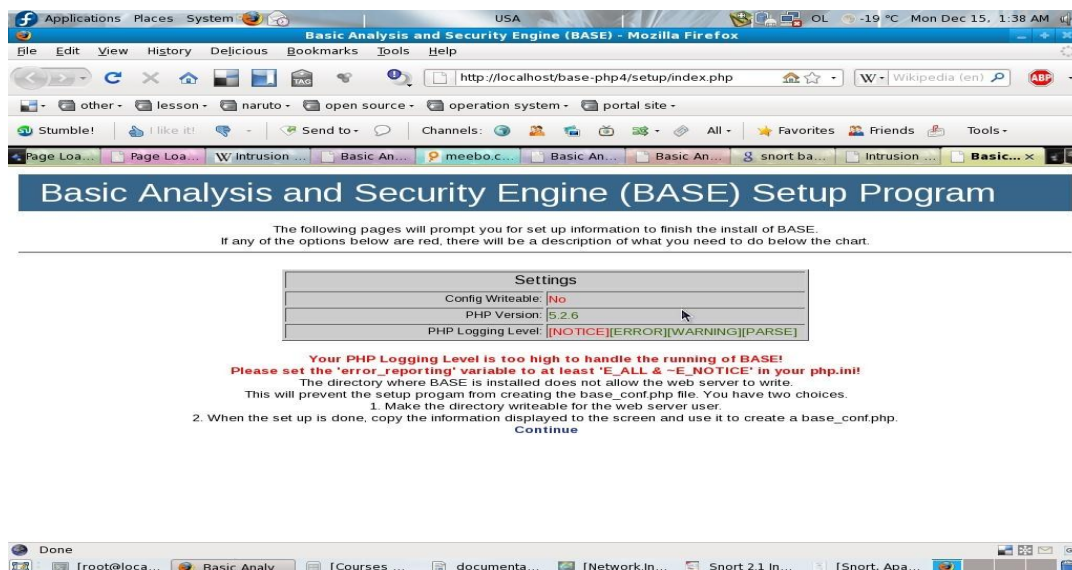
Эдгээр php хуудаснуудыг apache-аар ажиллуулахын тулд permission-ийг нь тохируулна. Гэхдээ энд owner нь apache group нь apache гэж тохируулсан байгаа нь жишээ бөгөөд аюулгүй байдал талаа анхаарахын тулд apache-ийн default хэрэглэгч болох apache-г owner нь болгон тохируулахгүй байхыг зөвлөж байна. Гэхдээ суулгах тухайн вэб сайтыг суулгахад apache хэрэглэгч нь base-ийн үндсэн тохиргооны файлд өөрчлөлт хийх учир permission-ийг нь apache хэрэглэгч write эрхтэй байхаар тохируулсан байх шаардлагатай. Харин суулгасныхаа дараа write эрхийг нь болиулна.

```
#chown -R apache:apache /var/www/html/base #chown -R apache:apache /var/www/html/adodb
```

BASE хуудсыг анх ажиллуулахад Зураг 3-т үзүүлсэн байдлаар directory –т эрх байхгүй байна гэсэн алдаа заах учир base -ийн direcotory-т бичих эрхийг нэмнэ. Дараах командаар бичих эрх нэмж болно.

```
#chmod o+w /var/www/html/base
```

Permission-ийг зөв тохируулсны дараа 5-н алхам дамжаад base-ийг /var/www/html/base ашиглах боломжтой болно.



Зураг 3. Base

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа

Алхам 1. Зураг 4-т үзүүлснээр хэлээ тохируулах болон өгөгдлийн сантайгаа



Step 1 of 5	
Pick a Language:	english [?]
Path to ADODB:	/var/www/html/adodb [?]
<input type="button" value="Submit Query"/>	

Зураг 4. ADODB зам (Нэгдүгээр алхам)

холбогдож ажилладаг ADODB-ийн замыг зааж өгнө.

Алхам 2. Зураг 5-д үзүүлсэн байдлаар өгөгдлийн сангийн төрөл, нэр, серверийн хаяг, порт, холбогдох нэр нууц үг зэрэг өмнө тохируулж байсан тохиргоонуудыг оруулна. Хэрэглэгчийн нэр, нууц үг зэрэг мэдээллүүдийг оруулна.

Step 2 of 5	
Pick a Database type:	MySQL [?]
Database Name:	snort
Database Host:	localhost
Database Port: Leave blank for default!	
Database User Name:	snort
Database Password:	нууц үг
<input type="checkbox"/> Use Archive Database [?]	
Archive Database Name:	
Archive Database Host:	
Archive Database Port: Leave blank for default!	
Archive Database User Name:	
Archive Database Password:	
<input type="button" value="Submit Query"/>	

Зураг 5. Өгөгдлийн сан (Хоёрдугаар алхам)

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа

Алхам 3. Зураг 6-д үзүүлснээр base хуудаснуудыг үзэхэд authentication хийдэг болгох тохиргооны хэсэг. Энд Administrator хэрэглэгчийн нэр, нууц үг зэрэг мэдээллүүдийг оруулна.

Step 3 of 5

☒ Use Authentication System [?]

Admin User Name: admin

Password: *****

Full Name: administrator

Submit Query

Зураг 6. (Гуравдугаар алхам)

Алхам 4. Зураг 7-д үзүүлснээр өгөгдлийн санд нэмэлт хүснэгтүүдийг үүсгэх хэсэг. Тэдгээр хүснэгтүүд нь халдлагад шинжилгээ хийхэд хэрэглэгдэнэ. “Create BASE AG” товчлуур дээр товшиж тэдгээр хүснэгтүүдийг үүсгэнэ.

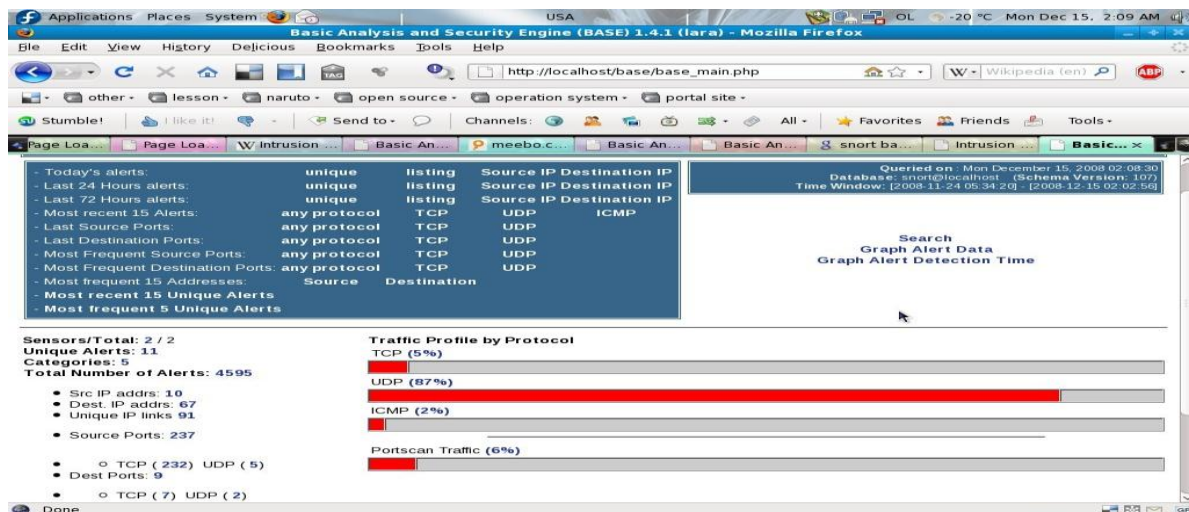
Step 4 of 5

Operation	Description	Status
BASE tables	Adds tables to extend the Snort DB to support the BASE functionality	Create BASE AG

• snort

Зураг 7. Өгөгдлийн сангийн нэмэлт

Алхам 5. Зураг 8-д үзүүлснээр үндсэн хуудас руу шилжиж уг хуудсыг шалгана.



Зураг 8. Хуудас шилжих

2.4 SNORT-ийг турших

Snort командаар Snort-ийг ажиллаж байгаа эсэхийг шалгана. Snort командыг ажиллуулахад дараах мэдээлэл гарч байвал Snort ажиллаж байна гэсэн үг.

```
$ Snort

-*> Snort! <*-

o" )~ Version 2.8.1 (Build 28)

"" By Martin Roesch & The Snort Team: http://www.Snort.org/team.html

(C) Copyright 1998-2008 Sourcefire Inc., et al. Using PCRE version: 7.8 2008-09-05

USAGE: Snort [-options] <filter options> Options:

-A

-b  Лог packets in tcpdump format (much faster!)

-B <mask> Obfuscated IP addresses in alerts and packet dumps using CIDR mask

-c <rules> Use Rules File <rules>

-C  Print out payloads with character data only (no hex)

-d  Dump the Application Layer

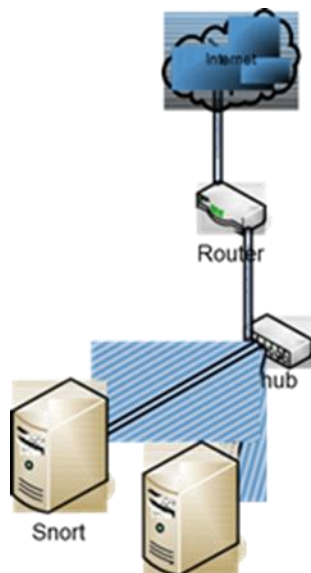
-D  Run Snort in background (daemon) mode

-e  Display the second layer header info

-f      Turn off fflush() calls after binary лог writes
```

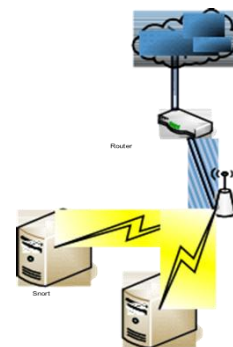
Snort командыг “-v” option-той ажиллуулж packet sniffer горимд ажиллаж байгаа эсэхийг шалгана. Хэрэв зөв ажиллаж байвал тухайн хостын хүлээн авсан болон дамжуулж байгаа, тухайн хостоор дамжиж байгаа пакетууд харагдана. Хэрэв decode хийж харахыг хүсвэл “d” option ашиглана.

Wireless access point ашиглан холбогдсон сүлжээний хувьд “Зураг 10”-д үзүүлснээр hub ашигласан сүлжээтэй адилаар Snort бүхий хост нь access point-той холбогдсон бол тухайн access point-оор дамжих пакетыг шинжлэх боломжтой болно.



Зураг 11. Switch ашигласан сүлжээ

Switch ашигласан сүлжээний хувьд “Зураг 11”-д үзүүлснээр Snort суусан хост руу сүлжээгээр дамжиж байгаа пакетуудыг дамжуулахын тулд port mirror хийх буюу нэг портоор дамжиж байгаа frame-үүдийг Snort суусан хостын холбогдсон порт руу хувилж дамжуулдаг болгоно. Тухайлбал үүний cisco-ийн managed switch-д span порт тохируулах замаар хэрэгжүүлж болно.



Зураг 10. Wireless Access point ашигласан сүлжээ

2.6. DoS халдлага зогсоож байгаа эсэхийг шалгах туршилт

Халдлага хийх хост дээр hping3 файлын багцыг суулгаж (fedora-д implement хийгдсэн байдаг учир “yum install hping3” командаар суулгах боломжтой) халдлага эсэргүүцэх систем бүхий хост руу дараах командыг ашиглан DoS халдлага хийж болно.

```
# hping3 -i u1 -S -p 80 -a 10.2.3.4 10.0.0.161
```

Энэхүү командыг бичиж өгснөөр халдлага эсэргүүцэх систем ажиллуулаагүй вэб сервер лүү халдлага хийхэд ойролцоогоор 2MB орчим пакетын урсгалаар вэб сервер дээрх apache service ажиллахгүй болдог байна. Өөрөөр хэлбэл халдлага хийгдэж байх үед дурын хостоос уг вэб серверийн вэбийг үзэж чадахгүй болно гэсэн үг.

Халдлага эсэргүүцэх систем халдлагыг таслан зогсоож байгаа эсэхийг iptables-т дүрэм нэмэгдэж байгаа эсэхээр нь мэдэж болно. Дараах командаар шалгаж болно.


```
# iptables -L
```

Chain INPUT (policy ACCEPT)	target	prot opt source	destination	
DROP		tcp -- 10.2.3.4	10.0.5.112	tcp
dpt:http				
Chain FORWARD (policy ACCEPT)	target	prot opt source	destination	
DROP		tcp -- 10.2.3.4	10.0.5.112	tcp
dpt:http				
Chain INPUT (policy ACCEPT)	target	prot opt source	destination	

Халдлага эсэргүүцэх систем ажиллаж байгаа вэб сервер лүү hping3-аар DoS халдлага хийж байх үед дурын хостоос вэб сервер дээрх вэб хуудсыг үзэж болж байна гэдэг нь халдлага эсэргүүцэх систем нь халдлагыг таслан зогсоож чадаж байна гэсэн үг юм.

2.7. Snort системийн гарын авлага

Дипломын ажлын хүрээнд Snort системийг ашиглах гарын авлага боловсруулж хавсралтад оруулсан.

<p>МОНГОЛ УЛСЫН БОЛОВСРОЛЫН ИХ СУРГУУЛЬ МАТЕМАТИК, БАЙГАЛИЙН УХААНЫ СУРГУУЛЬ</p> <p>МЭДЭЭЛЭЛ ЗҮЙН ТЭНХИМ</p> <p></p> <p>“SNORT ХАЛДЛАГА ИЛРҮҮЛЭХ СИСТЕМИЙН” ГАРЫН АВЛАГА</p> <p>Эмхтгэсэн: МБУС-ийн мэдээлэл зүйн тэнхимийн 4 курс оюутан Х.Хонгорцэдэг</p> <p>УЛААНБААТАР ХОТ 2020 ОН</p>	<p>МОНГОЛ УЛСЫН БОЛОВСРОЛЫН ИХ СУРГУУЛЬ МАТЕМАТИК, БАЙГАЛИЙН УХААНЫ СУРГУУЛЬ</p> <p>ГАРЧИГ</p> <p>Contents</p> <p>1.1. SNORT халдлага илрүүлэх, эсэргүүцэх систем 6</p> <p>1.2. SNORT халдлага илрүүлэх системийн үйл ажиллагааны зарчим 7</p> <p>1.2.1. SNORT халдлага илрүүлэх системийн дүрмийн синтакс 8</p> <p>1.3. SNORT халдлага илрүүлэх системийг суулгах 10</p> <p>1.3.1. SNORT халдлага илрүүлэх системийг тохируулах 11</p> <p>1.3.2. SNORT халдлага илрүүлэх систем дээр дүрэм нэмэх 12</p> <p>1.3.3. Deamon хэлбэрээр ажиллуулах тохиргоо 12</p> <p>1.3.4. Өгөгдлийн санд холбох тохиргоо 13</p> <p>1.3.5. Веб интерфэйстэй холбох 15</p> <p>1.4 SNORT-ийг турших 20</p> <p>1.5 SNORT халдлага илрүүлэх системийг байрлуулах 22</p> <p>1.6. DoS халдлага зогсоож байгаа эсхийг шалгах туршилт 23</p> <p>НОМ ЗҮЙ 24</p>
---	--

ДҮГНЭЛТ

Сүүлийн үеийн интернет сүлжээний хэрэглээ нь дан ганц суурин компьютерээр төдийгүй, гар утас зөөврийн төхөөрөмжүүдэд хамааралтай болон өсөн нэмэгдэж байна. Үүнийхээ хэрээр аюулгүй байдлаа хангаж, найдвартай ажиллагаатай байх асуудал чухлаар тавигдах болсон.

Энэ асуудлыг хангах нэг шийдэл бол халдлага илрүүлэх системийг ашиглах юм. Ихэнх халдлага илрүүлэх систем нь өндөр үнэтэй төхөөрөмж, ажиллагааны лиценз нь ч бас өндөр үнэтэй байдаг тул тэдгээр системүүдтэй адил түвшний гүйцэтгэлтэй нээлттэй эхийн SNORT халдлага илрүүлэх системийг ашиглах нь зөв шийдэл болох нь энэ ажлын үр дүн болно.

Уг халдлага эсэргүүцэх системийг ашиглах нь сүлжээгээр дамжих энгийн мэдээллүүдийн дамжих хурданд нөлөөлөхгүй байгаа учир үндсэн сүлжээний гарцан дээр ашигласан тохиолдолд сүлжээний хэвийн үйл ажиллагааг бууруулдаггүй байна.

Энэхүү төгсөлтийн ажлыг хийснээр сүлжээний халдлагууд, тэдгээрийн төрөл мөн сүлжээний халдлага илрүүлэх систем, халдлага эсэргүүцэх системүүдийн ялгааг судалж тогтоон онолын мэдлэгээ өргөтгөж тэлсэн байна. Мөн өргөн ашиглагддаг халдлага эсэргүүцэх, халдлага илрүүлэх хэрэгслүүдийг судалж тэдгээрээс дэлхий нийтээр хамгийн өргөн хэрэглэдэг Snort нээлттэй эхийн системийг судалж туршсанаараа давуу болсон гэж дүгнэж байна.

НОМ ЗҮЙ

1. Eyal Gruner, Нетанел Амар. (2015). *cynet.com* . Америк: платформ.
 2. wikipedia хөгжүүлэгч. (2016). *DoS халдлагууд*. Англи: платформ.
 3. Wikipedia хөгжүүлэгч нар . (2018). *Snort*. Англи: платформ.
 4. wikipedia хөгжүүлэгч нар. (2016). *Халдлага эсэргүүцэх систем*. Англи: платформ.
 5. wikipedia хөгжүүлэгчид. (2016). *Халдлага илрүүлэх систем*. Англи: платформ.
 6. Л.Мөнхбат. (2007). *Сүлжээний аюулгүй байдал хамгаалалт*. Улаанбаатар: платформ.
 7. Сэтгүүл . (2018). *Олон улсын аюулгүй байдлын инженерийн сэтгүүл*. Англи: платформ.
- <http://doc.emergingthreats.net/bin/view/Main/SnortSam>
 - <http://global-security.blogspot.com/2008/04/block-bad-oss-ips-with-content.html>

Хавсралт



МОНГОЛ УЛСЫН БОЛОВСРОЛЫН ИХ СУРГУУЛЬ МАТЕМАТИК, БАЙГАЛИЙН УХААНЫ СУРГУУЛЬ

МЭДЭЭЛЭЛ ЗҮЙН ТЭНХИМ



“SNORT ХАЛДЛАГА ИЛРҮҮЛЭХ СИСТЕМИЙН” ГАРЫН АВЛАГА

Эмхэтгэсэн: МБУС-ийн мэдээлэл зүйн тэнхимийн 4 курс оюутан Х.Хонгорцэцэг

ГАРЧИГ

Contents

1.1. SNORT халдлага илрүүлэх, эсэргүүцэх систем	31
1.2. SNORT халдлага илрүүлэх системийн үйл ажиллагааны зарчим.....	32
1.2.1. SNORT халдлага илрүүлэх системийн дүрмийн синтакс	33
1.3. SNORT халдлага илрүүлэх системийг суулгах	35
1.3.1. SNORT халдлага илрүүлэх системийг тохируулах.....	36
1.3.2. SNORT халдлага илрүүлэх систем дээр дүрэм нэмэх	36
1.3.3. Daemon хэлбэрээр ажиллуулах тохиргоо.....	37
1.3.4. Өгөгдлийн санд холбох тохиргоо.....	38
1.3.5. Вэб интерфейстэй холбох.....	39
1.4 SNORT-ийг турших	43
1.5 SNORT халдлага илрүүлэх системийг байрлуулах.....	44
1.6. DoS халдлага зогсоож байгаа эсэхийг шалгах туршилт	45
НОМ ЗҮЙ	46

ӨМНӨХ ҮГ

Сайн байцгаана уу.

МУБИС-ийн Математик, Байгалийн ухааны сургуулийн оюутан танд энэ өдрийн мэнд хүргэе

Мэдээллийн эрин зуун болсон өнөө үед, дэлхий нийтээрээ даяарчлал, хувьсгал, шинэчлэл өөрчлөлтийг ар араасаа хурдацтай хийсээр байна. Мэдээллийн технологи асар хурдтайгаар хөгжиж, хийсвэр оюун ухаан, робот, ИТ, сүлжээ зэрэг нь салбартаа тэргүүлсээр, улам боловсронгуй хөгжиж бидний зайлшгүй мэдэх ёстой боловсрол болсон байна.

Харилцаа холбооны хэрэгсэл аль ч цаг үед эн тэргүүнд байсан тэгвэл гар утас нь улам боловсронгуй болсоор виртуал орчинд хүртэл холбоо барьж түүнчлэн, дүрс бичлэг, дуу зэрэг төрөл бүрийн үйл ажиллагаа хийдэг. Яаж холбоо барих бэ? та сүлжээний асуудлаа шийдчихсэн байхад л хангалттай. Та гар утсандаа хамгаалалт хийж нууц үг оруулдаг шиг, сүлжээнд ч бас нууц үг хамгаалалт хийх хэрэгтэй. Сүлжээний халдлага газар авч хэрэгтэй мэдээллээ хэрхэн хадгалах талаар асуулт тулгарна. Сүлжээний халдлагын хамгийн том илрүүлэлт бол халдлага илрүүлэх систем юм.

Халдлага илрүүлэх систем нь өндөр үнэтэй төхөөрөмж, ажиллагааны лиценз нь үнэтэй байдаг бол тэдгээр системүүдтэй адил түвшний гүйцэтгэлтэй нээлттэй эхийн SNORT халдлага илрүүлэх системийг ашиглах нь зөв шийдэл юм.

1.1. SNORT халдлага илрүүлэх, эсэргүүцэх систем

Snort IPS нь хор хөнөөлтэй сүлжээний үйл ажиллагааг тодорхойлоход туслах хэд хэдэн дүрмийг ашигладаг бөгөөд тэдгээр дүрмүүдтэй тохирсон пакетуудыг хайж олоход хэрэглэгчдэд сэрэмжлүүлэг өгдөг.

Snort нь гурван үндсэн хэрэглээтэй: tcpdump шиг пакет үнэрлэгч, пакет бүртгэгч гэх мэт - сүлжээний траффик шалгахад тустай, эсвэл сүлжээний нэвтрэлтээс урьдчилан сэргийлэх систем болгон ашиглаж болно. Snort-ийг хувийн болон бизнесийн зорилгоор татаж авах, тохируулах боломжтой.

Snort нь IP сүлжээнд бодит хугацааны трафикийг шинжилгээ хийж пакетуудыг бүртгэдэг боломж бүхий сүлжээний халдлагыг илрүүлэх (NIDS) болон сүлжээний халдлагаас урьдчилан сэргийлэх (NIPS) нээлттэй эхийн үнэгүй систем юм.

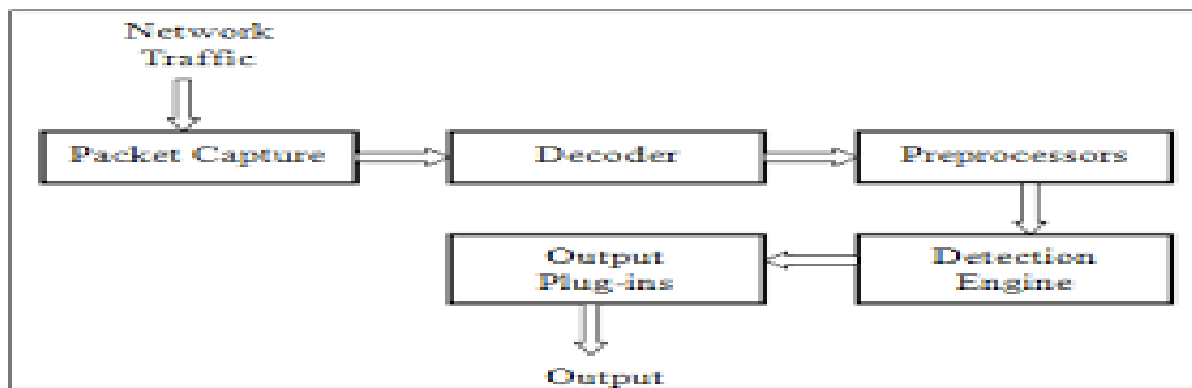
Snort нь протокол шинжилгээг хийж, агуулгаас хайлт хийхээс гадна OS fingerprint оролдлого, SMB судалгаа, вэб application довтолгоо, нэвтрэх боломжит порт шалгалтууд, буфер дүүргэлтийн алдаа шалгалт болон бусад халдлага, шинжлэгч нарыг пассив илрүүлэх, актив блоклоход ихэвчлэн хэрэглэгддэг хэрэгсэл юм⁶. (wikipedia хөгжүүлэгч нар, 2016) [5]

Unix төст системд libpcap буюу windows системд winpcap гэх сүлжээний траффикийг тодорхой форматтайгаар файлд хадгалдаг application programming interface ашиглан пакетуудыг барьдаг. Тухайлбал Snort нь packet sniffing горимд пакетыг уншиж байх үедээ pcap (Packet CAPture library)-ийг ашиглан Process Packet функцийг дуудаж ажиллуулан пакетыг бүтцээр нь задална. Дараа нь IDS горимд шилжин уг пакетыг шалгаж үнэлгээ дүгнэлт өгнө. Эцэст нь packet-лог горимд шилжин гаралтын plug-in-уудыг дуудаж ажиллуулах замаар alert-уудыг үүсгэдэг.

Ихэвчлэн бидний шалгахыг хүссэн пакетууд интернетээс ирдэг тул таны Snort мэдрэгч нь таны дотоод сүлжээг гадаад ертөнцөөс тусгаарлаж, периметр дээр байх болно. Мэдрэгчийг хаана байрлуулахыг хүсэж байна (жишээлбэл, галт хананы өмнө, дараа эсвэл дотор талд), энэ нь танаас хамаарна. Хэрэв та бүх траффикийг харахыг хүсвэл дараах схемийг баримтална уу: Internet> Router> Sensor> Firewall> Switch> Дотоод сүлжээ. Нөгөө талаас, хэрэв та мэдрэгчийг галт хананы өмнө байрлуулахыг хүсэж байвал галт ханаар дамжин өнгөрөх

⁶ Wikipedia link

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа хөдөлгөөнийг л харах боломжтой болно. Энэ тохиолдолд та Интернет> Чиглүүлэгч> Галт хана> Мэдрэгч> Шилжүүлэгч> Дотоод сүлжээ гэсэн схемийг дагаж мөрдөх болно. Snort мэдрэгчийг траффик хянахыг хүссэн газартаа байрлуулж болно..



Зураг 12. Snort халдлага илрүүлэх системийн үйл ажиллагааны зарчим. UMUC, 2012

Сүлжээний траффик нь "Пакет декодер" -оор дамжин өнгөрөх болно. Энэ нь PPP холболт, Ethernet (зэс эсвэл шилэн кабелийн) холболт юм. Пакет декодерын зорилго нь урьдчилан боловсруулагчдын багцыг бэлтгэх явдал юм.

"Урьдчилан боловсруулагч" нь урсгалыг хүлээн авдаг бөгөөд ингэснээр Snort урьдчилсан процессорын залгааснууд нь TCP урсгалыг дахин угсрах, IP defragmentation, статистик мэдээлэл цуглуулах эсвэл HTTP хүсэлтийг хэвийн болгох зэрэг маш нарийн түвэгтэй функцүүдийг гүйцэтгэх боломжийг олгодог. Та "spp_something.c" болон "spp_something.h" файлуудыг өөрчилж Snort preprocessor залгааснуудыг нэмж болно. Эцсийн үүрэг бол илрүүлэх хөдөлгүүрийн дүрмүүдтэй харьцуулахын тулд пакетуудыг өөрчлөх явдал юм. (Сэтгүүл , 2018) [6]

1.2. SNORT халдлага илрүүлэх системийн үйл ажиллагааны зарчим

Snort нь гарын үсэг дээр суурилсан NIDS / NIPS тул урьдчилан тогтоосон дүрмийг баримталдаг. Snort дүрмүүд нь хоёр хэсгээс бүрдэнэ. "Толгой" нь Snort-ийн хийх арга хэмжээг зааж өгнө. Үүнд дүрмийн үйл ажиллагааны талаарх бүртгэл, сэрэмжлүүлэх зэрэг хүчин зүйлс орно. Толгой хэсэгт Snort дүрмийн эх сурвалж, хүлээн авах болон илгээх IP хаяг, хүлээн авах портын дугаар, ашиглагдаж буй протокол зэргийг багтаасан хэсгийг агуулна. Snort дүрмийн хоёр дахь хэсэг нь "Сонголтууд" юм. Сонголтууд бол аюулгүй байдлын пакетэд юу багтдаг, snort дүрмийг пакеттай тааруулахад гарч ирэх мессежийг тодорхойлох боломжтой.

Толгой						Сонголтууд	
Дүрэм үйл ажиллагаа	Протокол	Илгээгч IP хаяг	Илгээгч порт	Урсгал чиглэл	Хүлээн авах IP хаяг	Хүлээн авах порт	Нэмэлт тест, гаралтын мессеж гэх мэт

1.2.1. SNORT халдлага илрүүлэх системийн дүрмийн синтакс

Snort нь орж ирсэн пакетыг хөнөөлтэй үйл ажиллагаа явуулах пакет мөн гэдгийг танихын тулд дүрэм ашигладаг. Дүрмүүдийг хэрхэн тохиромжтой бичсэнээс халдлага илрүүлэх систем нь халдлагыг оновчтой тодорхойлж мэдэгдэл гаргах нь хамаарна. Иймд дүрмүүдийг зөв сонгох нь чухал юм.

Дүрмийг өөрийн системд тохиромжтой байдлаар бичих шаардлагатай байдаг боловч Snort-ийг хөгжүүлдэг багаас зөвлөмж болгож өөрсдийнх нь гаргадаг дүрмүүдийг албан ёсны сайтдаа үнэгүй татах боломжтойгоор байрлуулсан байдаг.

Гэхдээ тухайн сайтад бүртгэгдээгүй хэрэглэгчид нэмэлт сайжруулалт хийгддэггүй дүрмүүдийг л татах боломжтой, бүртгэгдсэн хэрэглэгчид нь шинэ гарсан дүрмүүдийг 30 хоногийн дараанаас татах боломжтой болно, бүртгэгдээд төлбөр төлсөн хэрэглэгчид болон хөгжүүлэгчид нь шинэ дүрмийг гарсан дариуд нь авах боломжтой байдаг. Шинэ дүрэм гарахаараа бүртгэгдсэн хэрэглэгчдийн и-мэйл хаягаар нь мэдэгддэг.

Snort нь тодорхой синтаксийг дагаж мөрддөг. Энэ нь галт хананы дүрмүүдтэй төстэй боловч Options хэсэг нь галт хананаас илүү давуу тал болж өгдөг. Дүрмийн синтакс задаргааг нэг бүрчлэн доор тайлбарлав.

Дүрмийн үйл ажиллагаа: Энэ талбарт та бүртгэлийн, сэрэмжлүүлэх, дамжуулах, идэвхжүүлэх эсвэл динамик таван дүрмийн үйлдлүүдийн аль нэгийг нь сонгож болно. Хамгийн нийтлэг дүрмийн үйлдэл бол "сэрэмжлүүлэх" сонголт бөгөөд пакет болон хийсэн үйлдлийг бүртгэж дараа нь аюулгүй байдлын администраторт анхааруулга өгдөг.

Протокол: Энэ нь HTTP гэх мэт өндөр түвшний протокол, TCP, UDP, ICMP зэрэг доод түвшний протокол гэх мэт ашиглагдаж буй протоколыг тодорхойлдог. Та өөрийн тодорхой дүрмийг бий болгохын тулд аль алиныг нь сонгож болно.

Илгээгчийн IP хаяг: Энэ талбар нь пакетийг илгээгчийн хаяг юм. Энэ нь ганц IP хаяг эсвэл сүлжээний ID байж болно. Жишээлбэл, та ямар нэгэн илгээгч IP хаягаас ирэх бүх урсгалыг анхааруулахыг хүсвэл "any" -г ашиглаж болно.

Илгээгчийн порт хаяг: Энэ талбар нь пакетийн эх TCP эсвэл UDP порт юм. Дахин хэлэхэд, хэрэв та бүх 65,535 портыг зааж өгөхийг хүсвэл "any" -ийг ашиглаж болно.

Урсгал (Чиглэл): Энэ талбар нь ихэвчлэн "->" (чиглэлтэй сум) тэмдгийг ашиглан пакет урсгалын чиглэлийг тодорхойлдог.

Хүлээн авах IP хаяг: Энэ бол пакет руу очих зориулалттай газар юм. Энэ нь ганц IP хаяг, сүлжээний ID эсвэл "дурын" хаяг байж болно.

Хүлээн авах Port хаяг: Энэ бол пакет руу очих зориулалттай TCP эсвэл UDP порт юм. Энэ нь ганц IP хаяг, сүлжээний ID эсвэл "дурын" хаяг байж болно.

Сонголтууд: Өмнө дурьдсанчлан Snort-ийн гол ашиглах хэсэг Options хэсэгт байна. Snort дүрмийн сонголтууд нь дүрмийг өөрөө боловсронгуй болгоход тусалдаг.

Агуулга: Энэ бол пакет ачааны доторх мөрийн хэв маягийг олоход хэрэглэгддэг түлхүүр үг юм. Энэ нь ASCII, хоёртын эсвэл арван зургаатын форматтай байж болно. Жишээлбэл, хортой програмын зарим хэлбэр нь тодорхой хоёртын эсвэл арван зургаатын мөртэй байдаг. Хэрэв та энэ мөрийг мэддэг бол үүнийг энд зааж өгөх боломжтой бөгөөд хэрэв таны сүлжээнээс үүнийг олж мэдвэл Snort танд анхааруулах болно.

Офсет: Офсет түлхүүр үгийг пакет доторх тодорхой байтын дараа хайлтын эхлэлийг зааж өгөхөд ашиглаж болно. Жишээлбэл, хэрэв та пакет доторх тодорхой байтын дараа хайлтаа эхлүүлэхийг хүсвэл энд бичиж болно.

Гүн: Гүнзгий түлхүүр үг нь пакет доторх тодорхой байтаар хязгаарлагдах хайлтыг тодорхойлоход хэрэглэгддэг. Энэ нь Offset сонголттой төстэй;

Тохиолдол: Энэ нь хайлтын үед том, жижиг үсгийг ялгах эсэхийг тохируулах хэсэг юм.

Агуулгын жагсаалт: Энэ түлхүүр үг нь "нууц үг", "ssn" гэх мэт түлхүүр үг агуулсан тодорхой текст файлыг олоход хэрэглэгддэг. Жишээлбэл, Snort эдгээр түлхүүр үгсийн файлыг хайж олох боломжтой. Та Snort-г интернет хайлт хийхэд ашиглаж

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа болно гэдэгт би итгэж байна. Жишээлбэл, хэрэв хэрэглэгч "порно" гэсэн түлхүүр үгийг хайж байсан бол аюулгүй байдлын администраторт анхааруулга өгөх болно.

Тугууд: тугуудын түлхүүр үгийг TCP толгой хэсэгт байрлуулсан алга болсон эсвэл тохиромжгүй тугуудыг илрүүлэхэд ашиглаж болно. Заримдаа алга болсон тугууд нь портыг сканнердах эсвэл дайрах шинж тэмдэг болдог. [6]

Snort дүрмүүд нь халдлага, хор хөнөөлтэй үйл ажиллагааг илрүүлдэг. Та сэрэмжлүүлэх, бүртгэл хийх, холболтыг таслах гэх мэт тодорхой дүрмүүдийг бичиж болно. Дүрмүүд нь энгийн синтакстай байдаг. Түүнчлэн, та бүх дүрмийг тохиргооны файлд бичиж, өөр системд тохирох зүйлээ засах боломжтой.

Snort нь гурван өөр горимтой. Эдгээр горимууд нь;

- Пакет Sniffer
- Пакет бүртгэгч
- NIPDS (Сүлжээнд нэвтрэх, урьдчилан сэргийлэх системийг илрүүлэх систем)

1.3. SNORT халдлага илрүүлэх системийг суулгах

Snort-ийг windows систем дээр суулгахдаа www.Snort.org татаж аваад step-to-step байдлаар суулгаж болно харин unix төст системүүд дээр эх кодыг нь татаж аваад компайл хийх, rpm багцыг нь татаж аваад суулгах боломжтой. Харин fedora project-д Snort-ийг fedora-д зориулан тохиргоо хийсэн кодыг бэлдсэн байдаг учир Snort-ийг fedora дээр yum install командаар суулгах боломжтой байдаг. Иймд Snort-ийг зөвхөн халдлага илрүүлэх систем байдлаар ажиллуулах тохиолдолд install командаар суулгах нь тохиромжтой. Snort-ийн бүх холбоотой багцуудыг суулгах бол “yum install Snort*” гэсэн командаар суулгаж болно. Харин зөвхөн mysql өгөгдлийн санд alert болон лог-уудаа хадгалдаг байхаар ашиглах бол yum install “Snort Snort-mysql” гэсэн командаар суулгах нь тохиромжтой. Ингэсэн тохиолдолд зөвхөн Snort нь mysql өгөгдлийн сантай холбогдох гаралтын plugin-тайгаа л сууна.

```
[root@localхост /]# yum install Snort*
```

```
Installed: Snort.i386 0:2.8.1-4.fc9 Snort-bloat.i386 0:2.8.1-4.fc9 Snort-mysql.i386
0:2.8.1-4.fc9 Snort-mysql+flexresp.i386 0:2.8.1-4.fc9 Snort-plain+flexresp.i386 0:2.8.1-
4.fc9 Snort-postgresql.i386 0:2.8.1-4.fc9 Snort-postgresql+flexresp.i386 0:2.8.1-4.fc9
Snort-snmp.i386 0:2.8.1-4.fc9 Snort-snmp+flexresp.i386 0:2.8.1- 4.fc9
```

Dependency Installed: libprelude.i386 0:0.9.17.2-1.fc9 mysql-libs.i386 0:5.0.51a-1.fc9
postgresql-libs.i386 0:8.3.4-1.fc9

1.3.1. SNORT халдлага илрүүлэх системийг тохируулах

Халдлагыг зөв тодорхойлох болон хэрэгцээтэй мэдээллээ цуглуулах нь Snort-ийг хэр зэрэг тухайн системд тохирсон оновчтой тохируулга хийж чадсанаас хамаарна. Иймд Snort-ийг тохируулахдаа дүрэм сонгох, ямар горимд ажиллуулах, өгөгдлийн сан ашиглах эсэхийг оновчтой байдлаар сонгох шаардлагатай.

Snort-ийн үндсэн тохиргооны файл нь fedora-ийн хувьд /etc/Snort/Snort.conf файл байдаг. Энэ файл дотор дүрмүүдийг тодорхойлох, гадаад болон дотоод сүлжээг ялгах, өгөгдлийн сантай холбох, server-үүдийн хаягийг заах (тухайлбал dns query-ийг alert болгож гаргахгүйн тулд dns server ямар хаяг дээр байгааг тодорхойлдог) зэрэг үндсэн тохиргоог хийдэг.

1.3.2. SNORT халдлага илрүүлэх систем дээр дүрэм нэмэх

Snort нь орж ирсэн пакетыг хөнөөлтэй үйл ажиллагаа явуулах пакет гэдгийг танихын тулд дүрэм ашигладаг. Дүрмүүдийг хэрхэн тохиромжтой бичсэнээс халдлага илрүүлэх систем нь халдлагыг оновчтой тодорхойлж alert гаргах нь хамаарна. Иймд дүрмүүдийг зөв сонгох нь чухал байдаг.

Өөрийн тодорхойлсон болон татаж авсан дүрмүүдийг ашиглахын тулд Snort-ийн үндсэн тохиргооны файлд оруулах шаардлагатай. Өөрөөр хэлбэл Snort-ийн үндсэн тохиргооны файлд дүрмийг тодорхойлж байгаа бичлэгийг нэмэх эсвэл Snort-ийн албан ёсны сайтаас татаж авсан дүрмүүд байрлах замыг зааж өгч include командаар сонгосон дүрмүүдийг үндсэн тохиргооны файлд оруулах шаардлагатай. Анхны утгаараа Snort-ийн үндсэн тохиргооны файлд “var RULE_PATH/etc/Snort/rules” гэсэн байдлаар дүрмүүдийн байрлах замыг тодорхойлсон байдаг. Иймд татаж авсан дүрмүүдийг /etc/Snort/rules хавтсанд хуулаад үндсэн тохиргооны файл дээр include командаар оруулснаар тухайн дүрмийг ашиглах боломжтой болно.

Тухайлбал scan хийдэг дүрмийг татаж аваад /etc/Snort/rules хавтсанд хуулсан байлаа гэхэд /etc/Snort/Snort.conf файлд дараах бичлэгийг нэмэх ёстой.

```
include $Rule_PATH/scan.rule
```

1.3.3. Deamon хэлбэрээр ажиллуулах тохиргоо

Системийн администратор тухайн хугацаанд Snort-ийг команд ашиглан ажиллуулна гэдэг нь администратор командыг хийж ажиллуулж байгаа season- оо хаахад Snort мөн ажиллахгүй болох учир энэ нь тохиромжгүй үйлдэл бөгөөд deamon хэлбэрээр ажиллуулах нь тохиромжтой. Тухайлбал Snort суулгасан машин унтарч ассан ч ажилладаг байхаар тохируулах үед энэ тохиргоо нь хэрэглэгдэнэ.

/etc/init.d/Snort файл дотор Snort-ийг deamon хэлбэрээр ажиллахад шаардагдах тохиргоонуудыг хийнэ. Тухайлбал service-ийг ачаалахад Snort нь ямар option-той ажиллах вэ гэдгийг тохируулна. “-D” option нь daemon горимд ажиллана гэдгийн заана, “-u” ямар хэрэглэгчийн эрхээр ажиллана гэдгийг заана.

Тухайлбал /etc/init.d/Snortd файлыг доор үзүүлсэн байдлаар тохируулж болно.

```

case "$1" in start)
    echo -n "Starting Snort: " cd /var/лог/Snort
    daemon /usr/sbin/Snort -D $SNORT_OPTIONS -u $USER -g $GROUP \
    -i $INTERFACE -c /etc/Snort/Snort.conf touch /var/lock/subsys/Snort
    echo
    ;;
stop)
    echo -n "Stopping Snort: " killproc Snort
    rm -f /var/lock/subsys/Snort echo
    ;;
restart)
    $0 stop
    $0 start
    ;;
status)
    status Snort
    ;;
*)
    Echn "Usage: So {start|stop|restart|status}"exit 1
Esac
Exit 0

```


1.3.4. Өгөгдлийн санд холбох тохиргоо

Snort нь пакетыг барьж аваад хадгалах замаар их хэмжээний лог болон alert-ийг үүсгэдэг учир тэдгээрийг файлд хадгалсан байдлаар нь удирдан зохицуулах нь түвэгтэй байдаг энэ байдлыг шийдвэрлэхийн тулд өгөгдлийн сантай холбож тэдгээр лог болон alert-ийг ангилан хадгалдаг. Энэ ажилдаа Snort-ийг mysql-тэй холбож лог болон alert-уудыг нь өгөгдлийн санд хадгалдаг болгосон.

Ингэхийн тулд mysql-ийг суулгасан байх шаардлагатай. Хэрэв суулгаагүй бол fedora дээр yum install командаар суулгах боломжтой.

```
#yum install mysql mysql-server Installed: mysql-server.i386 0:5.0.51a-1.fc9 ,  
mysql- 5.0.51a-1.fc9.i386
```

Mysql-ийг суулгасны дараа mysql-ээ demon хэлбэрээр ажиллуулах

```
# service mysqld start
```

Mysql admin-ий нууц үгийг тохируулах

```
# mysqladmin -u root password [нууц үг]
```

Mysql рүү root хэрэглэгчийн эрхээр нэвтрэх # mysql -u root -p

Snort-д зориулан лог болон alert-ийг хадгалдаг өгөгдлийн сан үүсгэх

```
mysql> CREATE DATABASE Snort; Query OK, 1 row affected (0.12 sec)
```

Snort-ийн өгөгдлийн санд хандах хэрэглэгчийг үүсгэх болон тухайн хэрэглэгчийн тухайн өгөгдлийн санд хандах эрх болон нууц үгийг нь тодорхойлох

```
mysql> grant all privileges on Snort.* to Snortusr@"localхост" identified by 'нууц үг';
```

```
Query OK, 0 rows affected (0.00 sec)
```

Өмнө хийсэн командыг идэвхжүүлэх.

```
mysql> flush privileges; Query OK, 0 rows affected (0.00 sec)
```

Үүсгэсэн өгөгдлийн сандаа лог болон alert хадгалахад хэрэглэгдэх хүснэгтүүдийг нэмэх. Yum install командаар Snort-ийг суулгах үед /usr/share/doc/Snort-2.8.1/create_mysql файл хуулагдсан байдаг. Уг файл нь хүснэгтүүдийг өгөгдлийн санд дараах командаар оруулж болно.

```
#mysql -u root -p < /usr/share/doc/Snort-2.8.1/create_mysql Snort
```

Snort-ийг өгөгдлийн сантай холбохдоо үндсэн тохиргооны файл дээр нь дараах бичлэгийг нэмнэ. Энэ бичлэг нь Snort-ийг өгөгдлийн сантайгаа холбогдоход нь хэрэглэгдэх тохиргоо бөгөөд өмнө нь суулгасан Snort-mysql plugin-ийг тохируулж байна гэсэн үг. Тухайлбал лог эсвэл alert-ийн алийг нь хадгалахыг заах, өгөгдлийн сангийн төрөл (mysql, mssql, postgresql-ийн аль нь гэдгийг), өгөгдлийн санд хандахад хэрэглэгдэх хэрэглэгчийн нэр болон нууц үг зэргийг тодорхойлсон байна. Тухайлбал дараах байдлаар бичиж оруулна. output database: лог, mysql, user=Snort password=нууц үг dbname=Snort хост=localhost

1.3.5. Вэб интерфейстэй холбох

Snort-ийн command line интерфейсийг хэрэглэх нь өргөн боломжтой байдаг боловч хэрэглэхэд түвэгтэй байдаг. Иймд вэб интерфейс холбож өгөгдлийн санд хадгалагдсан лог болон alert-ууд дээр задлан шинжилгээ хийх боломжтой.

Snort-д холбох боломжтой base болон acid зэрэг вэб интерфейс буюу php site-ууд байдаг. Энэ туршилтын ажлаараа би base-ийг суулгасан. Учир нь base нь acid-аас илүү хэрэглэх өргөн боломжтой байдаг. Тухайлбал acid нь alert-уудыг цагийн бүсээр нь ангилж үзүүлдэггүй.

Php хуудаснуудыг ажиллуулахдаа apache болон php-ийг суулган ажиллуулж болно. Тэдгээрийг fedora дээр дараах байдлаар yum install командаар суулгаж болно.

```
#yum install httpd php php-mysql
```

Вэб интерфейсийг холбохын тулд дараах php site-уудыг татаж авна.

- Base:

http://sourceforge.net/project/showfiles.php?group_id=103348&package_id=128846&release_id=617636

- ADODB: <http://phplens.com/lens/dl/adodb453.tgz>

Эдгээр нь adodb*.tgz болон base.tar.gz файлууд байх бөгөөд тэдгээрийг задлаад вэб сервер ажиллаж байгаа directory-т хуулна. Тухайлбал дараах командуудыг ашиглан хуулж болно.

```
$tar -xvzf ~/adodb453.tgz
$mv ~/adodb453 /var/www/html/adodb
$tar -xvf ~/base-1.4.1.tar.gz
$mv ~/base-php4 /var/www/html/base
```

Эдгээр php хуудаснуудыг apache-аар ажиллуулахын тулд permission-ийг нь

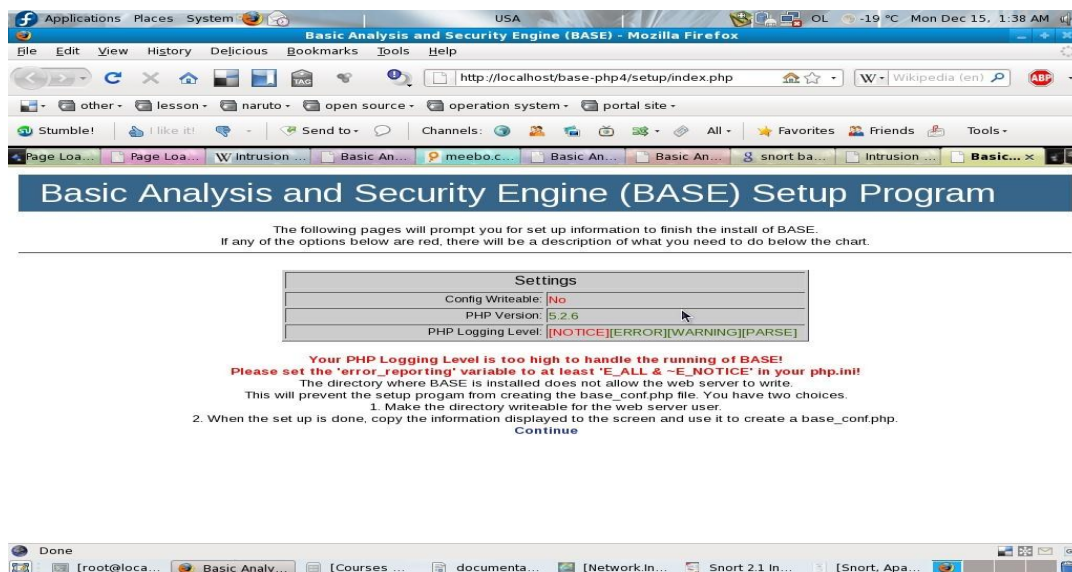
Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа тохируулна. Гэхдээ энд owner нь apache group нь apache гэж тохируулсан байгаа нь жишээ бөгөөд аюулгүй байдал талаа анхаарахын тулд apache-ийн default хэрэглэгч болох apache-г owner нь болгон тохируулахгүй байхыг зөвлөж байна. Гэхдээ суулгах тухайн вэб сайтыг суулгахад apache хэрэглэгч нь base-ийн үндсэн тохиргооны файлд өөрчлөлт хийх учир permission-ийг нь apache хэрэглэгч write эрхтэй байхаар тохируулсан байх шаардлагатай. Харин суулгасныхаа дараа write эрхийг нь болиулна.

```
#chown -R apache:apache /var/www/html/base #chown -R apache:apache /var/www/html/adodb
```

BASE хуудсыг анх ажиллуулахад Зураг 3-т үзүүлсэн байдлаар directory –т эрх байхгүй байна гэсэн алдаа заах учир base -ийн directory-т бичих эрхийг нэмнэ. Дараах командаар бичих эрх нэмж болно.

```
#chmod o+w /var/www/html/base
```

Permission-ийг зөв тохируулсны дараа 5-н алхам дамжаад base-ийг /var/www/html/base ашиглах боломжтой болно.



Зураг 13. Base

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа

Алхам 1. Зураг 4-т үзүүлснээр хэлээ тохируулах болон өгөгдлийн сантайгаа

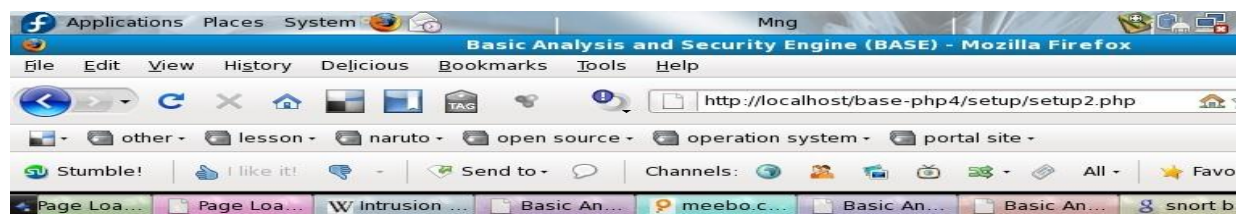


Step 1 of 5	
Pick a Language:	english [?]
Path to ADODB:	/var/www/html/adodb [?]
<input type="button" value="Submit Query"/>	

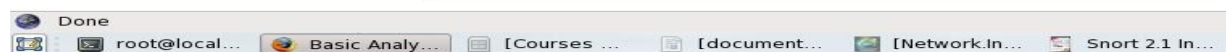
Зураг 14. ADODB зам (Нэгдүгээр алхам)

холбогдож ажилладаг ADODB-ийн замыг зааж өгнө.

Алхам 2. Зураг 5-д үзүүлсэн байдлаар өгөгдлийн сангийн төрөл, нэр, серверийн хаяг, порт, холбогдох нэр нууц үг зэрэг өмнө тохируулж байсан тохиргоонуудыг оруулна. Хэрэглэгчийн нэр, нууц үг зэрэг мэдээллүүдийг оруулна.



Step 2 of 5	
Pick a Database type:	MySQL [?]
Database Name:	snort
Database Host:	localhost
Database Port: Leave blank for default!	
Database User Name:	snort
Database Password:	нууц үг
<input type="checkbox"/> Use Archive Database [?]	
Archive Database Name:	
Archive Database Host:	
Archive Database Port: Leave blank for default!	
Archive Database User Name:	
Archive Database Password:	
<input type="button" value="Submit Query"/>	



Зураг 15. Өгөгдлийн сан (Хоёрдугаар алхам)

Сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх системийн судалгаа

Алхам 3. Зураг 6-д үзүүлснээр base хуудаснуудыг үзэхэд authentication хийдэг болгох тохиргооны хэсэг. Энд Administrator хэрэглэгчийн нэр, нууц үг зэрэг мэдээллүүдийг оруулна.

Step 3 of 5

☒ Use Authentication System [?]

Admin User Name: admin

Password: *****

Full Name: administrator

Submit Query

Зураг 16. (Гуравдугаар алхам)

Алхам 4. Зураг 7-д үзүүлснээр өгөгдлийн санд нэмэлт хүснэгтүүдийг үүсгэх хэсэг. Тэдгээр хүснэгтүүд нь халдлагад шинжилгээ хийхэд хэрэглэгдэнэ. “Create BASE AG” товчлуур дээр товшиж тэдгээр хүснэгтүүдийг үүсгэнэ.

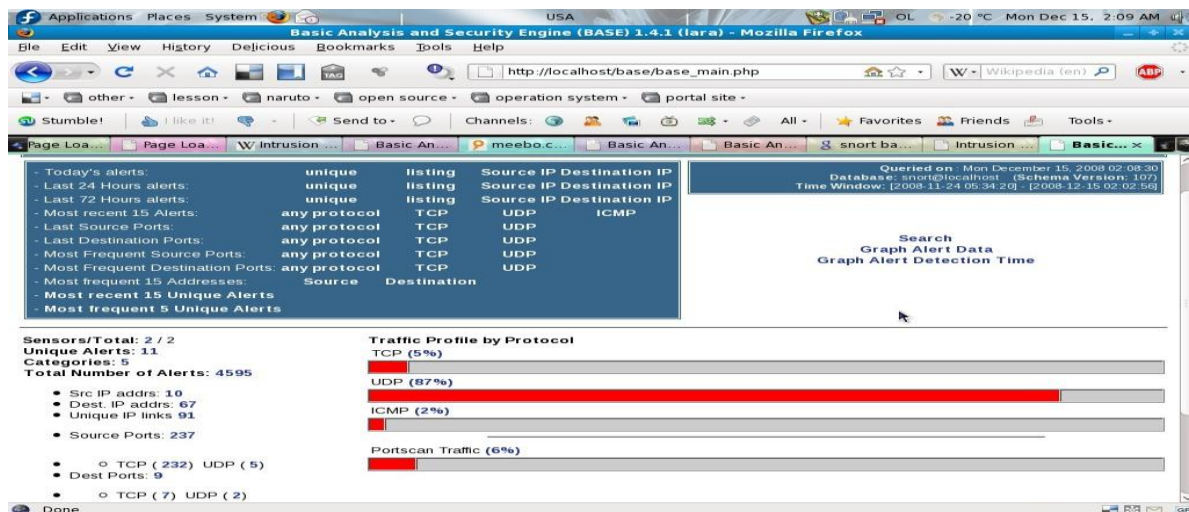
Step 4 of 5

Operation	Description	Status
BASE tables	Adds tables to extend the Snort DB to support the BASE functionality	Create BASE AG

- snort

Зураг 17. Өгөгдлийн сангийн нэмэлт

Алхам 5. Зураг 8-д үзүүлснээр үндсэн хуудасруу шилжиж уг хуудсыг шалгана.



Зураг 18. Хуудас шилжих

1.4 SNORT-ийг турших

Snort командаар Snort-ийг ажиллаж байгаа эсэхийг шалгана. Snort командыг ажиллуулахад дараах мэдээлэл гарч байвал Snort ажиллаж байна гэсэн үг.

```
$ Snort

-*> Snort! <*-

o" )~ Version 2.8.1 (Build 28)

"" By Martin Roesch & The Snort Team: http://www.Snort.org/team.html

(C) Copyright 1998-2008 Sourcefire Inc., et al. Using PCRE version: 7.8 2008-09-05

USAGE: Snort [-options] <filter options> Options:

-A

-b  Лог packets in tcpdump format (much faster!)

-B <mask> Obfuscated IP addresses in alerts and packet dumps using CIDR mask

-c <rules> Use Rules File <rules>

-C  Print out payloads with character data only (no hex)

-d  Dump the Application Layer

-D  Run Snort in background (daemon) mode

-e  Display the second layer header info

-f      Turn off fflush() calls after binary лог writes
```

Snort командыг “-v” option-той ажиллуулж packet sniffer горимд ажиллаж байгаа эсэхийг шалгана. Хэрэв зөв ажиллаж байвал тухайн хостын хүлээн авсан болон дамжуулж байгаа, тухайн хостоор дамжиж байгаа пакетууд харагдана. Хэрэв decode хийж харахыг хүсвэл “d” option ашиглана.

```
# Snort -v

Not Using PCAP_FRAMES

12/15-00:29:26.815460 10.0.5.217:137 -> 10.0.5.255:137

UDP TTL:128 TOS:0x0 ID:31 IpLen:20 DgmLen:96

Len: 68

+++++
+++++

12/15-00:29:27.565365 10.0.5.217:137 -> 10.0.5.255:137

UDP TTL:128 TOS:0x0 ID:32 IpLen:20 DgmLen:96

Len: 68

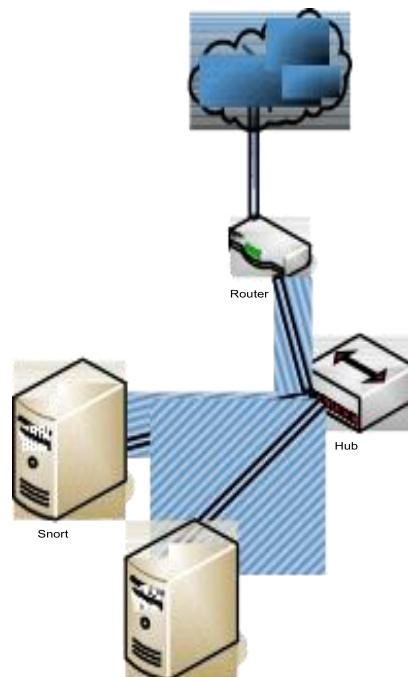
+++++
+++++
```

1.5 SNORT халдлага илрүүлэх системийг байрлуулах

Snort нь Network-based Intrusion Detection System учир шинжилгээ хийх сүлжээний пакетууд дамжих байрлалд буй хост дээр суусан байх шаардлагатай. Өөрөөр хэлбэл Snort нь тухайн сүлжээнд шинжилгээ хийхийн тулд пакетын урсгал төвлөрсөн газар байрлах ёстой.

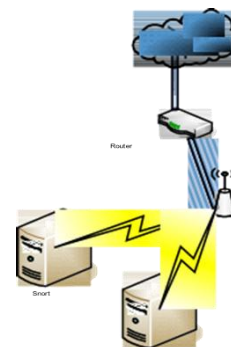
Тухайлбал Snort суусан машин нь төв тухайн сүлжээний төв шугамд холбогдсон байвал тухайн сүлжээгээр дамжиж байгаа пакетуудад шинжилгээ хийхэд тохиромжтой.

Hub ашиглан холбогдсон сүлжээний хувьд “Зураг 9”-д үзүүлснээр Snort суусан хостийг hub-ийн аль нэг портонд холбоход тухайн hub-аар дамжиж байгаа бүх пакетуудад шинжилгээ хийх боломжтой болно.

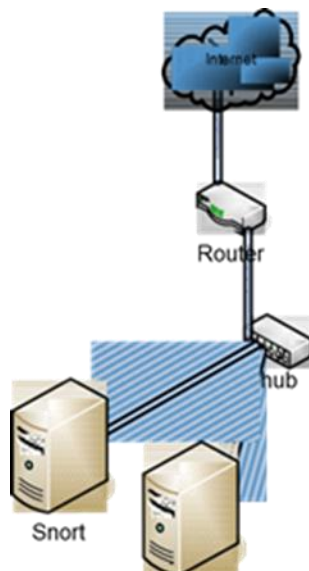


Зураг 19. Нив ашигласан сүлжээ

Wireless access point ашиглан холбогдсон сүлжээний хувьд “Зураг 10”-д үзүүлснээр hub ашигласан сүлжээтэй адилаар Snort бүхий хост нь access point-той холбогдсон бол тухайн access point-оор дамжих пакетыг шинжлэх боломжтой болно.



Зураг 20. Wireless Access point ашигласан сүлжээ



Зураг 21. Switch ашигласан сүлжээ

Switch ашигласан сүлжээний хувьд “Зураг 11”-д үзүүлснээр Snort суусан хост руу сүлжээгээр дамжиж байгаа пакетуудыг дамжуулахын тулд port mirror хийх буюу нэг портоор дамжиж байгаа frame-үүдийг Snort суусан хостын холбогдсон порт руу хувилж дамжуулдаг болгоно. Тухайлбал үүний cisco-ийн managed switch-д span порт тохируулах замаар хэрэгжүүлж болно.

1.6. DoS халдлага зогсоож байгаа эсэхийг шалгах туршилт

Халдлага хийх хост дээр hping3 файлын багцыг суулгаж (fedora-д implement хийгдсэн байдаг учир “yum install hping3” командаар суулгах боломжтой) халдлага эсэргүүцэх систем бүхий хост руу дараах командыг ашиглан DoS халдлага хийж болно.

```
# hping3 -i u1 -S -p 80 -a 10.2.3.4 10.0.0.161
```

Энэхүү командыг бичиж өгснөөр халдлага эсэргүүцэх систем ажиллуулаагүй вэб сервер лүү халдлага хийхэд ойролцоогоор 2MB орчим пакетын урсгалаар вэб сервер дээрх apache service ажиллахгүй болдог байна. Өөрөөр хэлбэл халдлага хийгдэж байх үед дурын хостоос уг вэб серверийн вэбийг үзэж чадахгүй болно гэсэн үг.

Халдлага эсэргүүцэх систем халдлагыг таслан зогсоож байгаа эсэхийг iptables-т дүрэм нэмэгдэж байгаа эсэхээр нь мэдэж болно. Дараах командаар шалгаж болно.

```
# iptables -L
```

Chain INPUT (policy ACCEPT)				destination	
target	prot	opt	source		
DROP	tcp	--	10.2.3.4	10.0.5.112	tcp
dpt:http					

Chain FORWARD (policy ACCEPT) target		
DROP	prot opt source tcp -- 10.2.3.4	destination 10.0.5.112
dpt:http		tcp
Chain INPUT (policy ACCEPT)		
target prot opt source	destination	

Халдлага эсэргүүцэх систем ажиллаж байгаа вэб сервер лүү hping3-аар DoS халдлага хийж байх үед дурын хостоос вэб сервер дээрх вэб хуудсыг үзэж болж байна гэдэг нь халдлага эсэргүүцэх систем нь халдлагыг таслан зогсоож чадаж байна гэсэн үг юм.

НОМ ЗҮЙ

1. Eyal Gruner, Нетанел Амар. (2015). *cyneet.com* . Америк: платформ.
 2. wikipedia хөгжүүлэгч. (2016). *DoS халдлагууд*. Англи: платформ.
 3. Wikipedia хөгжүүлэгч нар . (2018). *Snort*. Англи: платформ.
 4. wikipedia хөгжүүлэгч нар. (2016). *Халдлага эсэргүүцэх систем*. Англи: платформ.
 5. wikipedia хөгжүүлэгчид. (2016). *Халдлага илрүүлэх систем*. Англи: платформ.
 6. Л.Мөнхбат. (2007). *Сүлжээний аюулгүй байдал хамгаалалт*. Улаанбаатар: платформ.
 7. Сэтгүүл . (2018). *Олон улсын аюулгүй байдлын инженерийн сэтгүүл*. Англи: платформ.
- <http://doc.emergingthreats.net/bin/view/Main/SnortSam>
 - <http://global-security.blogspot.com/2008/04/block-bad-oss-ips-with-content.html>