Сигнатурт Тулгуурласан Сүлжээний Халдлага Илрүүлэх Систем Хөгжүүлэх нь

Б. Пүрэв-Очир
ШУТИС, КТМС, КУСалбар
Улаанбаатар, Монгол
purevochirb@yahoo.com

Ч. Эрдэнэбат
ШУТИС, КТМС, КУСалбар
Улаанбаатар, Монгол
ch.erdenebat@must.edu.mn

***Хураангуй*—Судалгааны ажлын хүрээнд хөгжүүлсэн систем нь тухайн хост дээр хяналт хийх бөгөөд сигнатурт тулгуурласан илрүүлэлтийн аргачлал ашиглах замаар халдлагыг илрүүлнэ. Систем нь тодорхой тооны сигнатурын сантай ба програмчлалын Си хэл болон түүний libpcap тусгай санг ашигласан болно.**

***Түлхүүр үг*—сигнатур, халдлага илрүүлэх систем, пакет, паттерн, ХИС;**

I. Оршил

Мэдээлэл холбооны технологийн эрчимт хөгжлийн хурдцыг дагаад өнөө үед цахим гэмт хэргийн арга хэрэгсэл нарийсч, гаралтын тоо давтамж өссөөр байна [1].

Мэдээллийн аюулгүй байдал нь мэдээлэл ба мэдээллийн системд зөвшөөрөлгүй хандах, мэдээллийг ашиглах, ил болгох, өөрчлөх, хуулах, устгах, системийн үйл ажиллагааг тасалдуулах, хянах ... зэрэг аюул заналуудаас хамгаалахыг хэлнэ [2]. Хэрэв таны компьютер интернетгүй, сүлжээгүй орчинд ажилладаг бол гадны халдлагаас айх зүйл үгүй юм. Харин интернет хэмээх задгай ертөнцөд байрлах мэдээлэл болон компьютерийн хувьд бол нууцлал хамгааллын асуудал хурцаар тавигдана. Иймд, мэдээллийн нууцлал, сүлжээний аюулгүй байдлыг хангах нь мэдээллийн аюулгүй байдлын нэн тэргүүний зорилго юм [3].

Сүлжээний халдлага нь хорт програм буюу довтлогч этгээдээс цохож авсан бай руу хийж буй дайралт мөн. Сүлжээний аюулгүй байдлыг тодорхойлж, халдлагын шинж чанарыг судлан, загварчлах замаар олж авсан мэдлэг дээр тулгуурлан халдлагын тодорхойлолт буюу сигнатурыг аюулгүй байдлын мэргэжилтнүүд гаргаж авдаг.

II. Судлагдсан байдал

Монгол улсад сүлжээний аюулгүй байдал, халдлага илрүүлэх системийн талаар сүүлийн үед нилээдгүй яригддаг боловч яг энэ талаар судалсан хэрэгжүүлсэн зүйлс бага байна.

Багш Г. Гандэмбэрэл, судлаач С. Отгонлхагва нар халдлага эсэргүүцэх системийн тухай зарим туршилт судалгаа хийсэн [4] бөгөөд тэд нээлттэй эхийн *Snort* системийг диамонд хэлбэрээр ажиллуулж туршсан байдаг.

Мөн, судлаач Б. Бямбадорж нь Ө. Эсболд профессорын удирдлага дор утасгүй сүлжээний халдлага илрүүлэх системийн талаар судалгааны ажил хийж гүйцэтгэсэн [5] ба утасгүй сүлжээний рүүтер дээр сүлжээний бүх урсгалыг нээлттэй эхийн *Snort* [6] системийг суулгаж, тохируулсан компьютер руу чиглүүлэлт хийх програм бичих замаар хэрэгжүүлсэн байдаг.

Халдлага илрүүлэх системийг эхнээс нь загварчлан хөгжүүлэлт хийж байгаа нь манай судалгааны ажлын онцлог тал юм.

III. Халдлага илрүүлэх систем

Сүүлийн жилүүдэд кибер халдлагын тоо, давтамж огцом өсөж байгаа бөгөөд үүнийг илрүүлэх нь мэдээллийн технологийн аюулгүй байдлын голлох чиг хандлага болж байна. Халдлага илрүүлэх системийн (ХИС) гол зорилго нь болзошгүй аюул заналхийлэлд бэлтгэлтэй байж тэдгээрийг илрүүлэн мэдээлэхэд оршино. Сүлжээний халдлага гэдэг нь сүлжээний хэвийн байдлыг алдагдуулах, холболтыг таслах, өөрчлөх болон холболтыг барьцаалах ... г.м. тодорхой хэв шинжүүдтэй байдаг.

Халдлага илрүүлэх системүүдийг ерөнхийдөө суурилах хүрээгээр нь 2 ангилж авч үздэг.

A. Сүлжээнд суурилсан халдлага илрүүлэх систем

Сүлжээнд суурилсан халдлага илрүүлэх системийн (СХИС) ажиллагааны зарчим нь сүлжээний рүүтер эсвэл хостын түвшний пакетуудын мэдээлэлд анализ болон бүртгэл хийх замаар сэжигтэй пакетуудыг илрүүлж, дэлгэрэнгүй мэдээллийг нь лог файл руу бичдэг. Энэхүү аргачлал нь өмнө мэдэгдсэн сүлжээний халдлагуудын шинж тэмдэгүүдээр (сигнатур) бүрдүүлсэн өгөгдлийн санг ашиглан пакет бүрийг нарийвчилан шалгадаг байна. Энэ төрлийн зарим ХИС нь хэрэв халдлага илэрвэл системийн аюулгүй байдлын багийн гишүүдэд сануулгын е-мэйл илгээнэ [7].

B. Хостод суурилсан халдлага илрүүлэх систем

Хостод суурилсан халдлага илрүүлэх систем (ХХИС) нь дотоод сүлжээн дэх тухайн нэг компьютерийг хянах замаар хэрэгждэг. Халдлагыг

илрүүлэх болон шалгахдаа системийн үйл ажиллагааны лог файлаас халдлагыг хайдаг. Хэрэв ямар нэгэн дүрмийн бус үйл ажиллагаа болох зөвшөөрөлгүй хандалт, амжилтгүй хандалт зэрэг нь лог файлаас илэрвэл дохиоллын системийг идэвхижүүлж систем халдлагад өртөж байгааг мэдээлнэ [8].

IV. Илрүүлэлтийн арга

ХИС –ийн ажиллагаа нь илрүүлэлтийн хөдөлгүүр дээр суурилж хэрэгжинэ. Илрүүлэлтийн хөдөлгүүр нь ерөнхийдөө 2 үндсэн аргад тулгуурлан хөгждөг байна.

A. Сигнатурт тулгуурласан илрүүлэлт

Систем нь халдлагын тодорхойлолт болох олон тооны сигнатураар тоноглогдсон байна. Халдлагыг илрүүлэхдээ сүлжээний урсгалийг сигнатурын сантай тулгалт хийдэг. Тодорхойлогдсон загвар буюу сигнатур нь ерөнхийдөө дараалсан эсвэл модон бүтэцтэй байна. Дарааллын загвар нь ихэнхидээ жирийн илэрхийллүүд байдаг. Модон бүтэцтэй паттерны загвар нь өгөгдлийн мод бүтцийг ашиглан хөгжүүлэгддэг тул бүтээмж нь харьцангуй өндөр байдаг.

Хамгийн энгийн паттерн тулгалтын загвар бол хувьсагчийн нээлттэй утга юм. Жишээ нь, энгийн функцийг авч үзье.

```
f 0 = 1
```

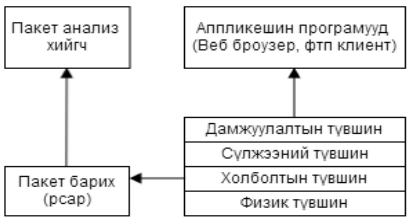
Дээрх илэрхийллийн 0 бол эхний паттерний утга юм. F өгөгдөл 0 аргументтэй паттернтэй тулах юм бол функц 1 гэсэн утгыг буцаана. Өөр ямар нэгэн утгатай аргументтэй тулвал функц амжилтгүй болно [9].

B. Аномалид суурилсан илрүүлэлт

Машины өгөгдөл олборлолтыг судлаж системийн хэвийн байдлын загваруудыг үүсгэнэ. Загвараас тодорхой утгаар хазайж байвал хэвийн бус (аномали) гэж үзэх замаар илрүүлэлтийг хэрэгжүүлдэг. Давуу тал нь өмнө нь үзэгдээгүй халдлагийг илрүүлнэ. Харин, сул тал нь ихээхэн хэмжээний хуурамч илрүүлэлтийн дохио өгөх ба динамик орчинд системийг загварчлахад хүндрэлтэй байдаг [10].

V. Хэрэгжүүлэлт

Судалгааны ажлын програмыг бичихдээ бид стандарт Си хэл болон түүний тусгай libpcap санг ашигласан. Libpcap нь доод түвшний сүлжээний хяналт хийх боломж олгогч сан юм. Уг сан нь сүлжээний статистикийн цуглуулга, аюулгүй байдлын шалгалт болон сүлжээний доголдлын илрүүлэлт ... зэрэг олон хэрэглээтэй. Libpcap –ын зохиогчид систем үл хамаарах API –ийг үүсгэсэн нь өмнө нь үйлдлийн системээс өндөр хамааралтай байсан пакет барих ажиллагааг эрс хөнгөвчилсөн. Хэрэв доод түвшний сүлжээний урсгалд хяналт хийх шаардлага гарвал libpcap –ийг ашиглах нь маш үр дүнтэй юм [11].

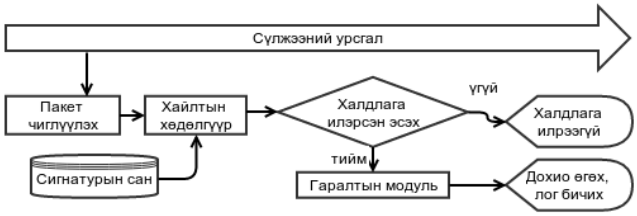


Зураг 1. OSI түвшиний pcap пакет баригч

Манай систем нь одоогоор нийтлэг халдлагууд болох DoS [12] болон түүний төрлийн халдлагуудыг илрүүлж байгаа. Уг систем нь үндсэн дөрвөн хэсгээс бүрдэнэ. Үүнд:

- Сүлжээний урсгалыг цуглуулах;
- Тодорхой порт, протокол, хаяг дээр шүүлт хийх;
- Пакетийн урсгалыг дүрэмтэй тулгах;
- Сэжигтэй пакетуудын лог мэдээллийг бичих;

Систем ачаалсаны дараа мэдрэгч ажиллаж эхлэх бөгөөд шаардлагатай порт, протокол эсвэл IP хаяг дээр шүүлт хийх боломжтой. Хүссэн пакетын урсгалыг системдээ оруулж ирсэний дараа эдгээр пакетууд илрүүлэлтийн хөдөлгүүрээр дамжих ба хэрэв халдлагын сигнатуртай тулсан хэв шинжийг агуулсан байвал үүнийг халдлага хэмээн үзэж гаралтын модуль руу шилжих замаар анхааруулах дохио өгөх буюу лог файлд мэдээллийг бичнэ.



Зураг 2. Системийн архитектур

ХИС –ийн гол зүйлсийн нэг нь халдлагын тодорхойлолт буюу сигнатур юм. Сигнатурын санг үүсгэхдээ илрүүлэх гэж буй халдлагуудаа тодорхойлж халдлагыг гүйцэтгэн сүлжээний пакет баригч Wireshark програмаар [13] халдлагын пакетуудыг барьж авна. Дараа нь бариж авсан пакетууд дээрээ анализ хийн халдлагын тодорхойлолтыг гарган авна.

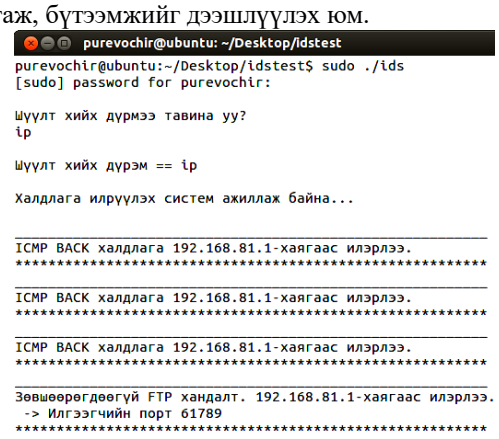
DoS –ын төрлийн SYN-Flood халдлагыг тодорхойлохдоо хостын сүлжээний карт дээр орж ирж буй TCP пакетуудын SYN флагийг тоолууртаа нэмэх ба харин орж ирж буй ACK флагийг энэ тоолууртаасаа хасах юм. Учир нь TCP нь найдвартай дамжуулалтын протокол тул дамжуулалт хийж байх үед SYN пакетын араас хүлээж авсан гэж мэдэгдэх ACK флагийг явуулдаг юм. Хэрэв энэ тоолуур 100,000 –аас дээш хэтэрвэл үүнийг SYN-Flood халдлага гэж тодорхойлох юм.

ICMP-Back халдлага нь хохирогчийн бродкаст хаяг руу их хэмжээний ping илгээх бөгөөд ингэснээр хохирогч талын компьютер энэ ping –ийг хүлээн авч

бродкаст хаяг руу хариу ping илгээх ба энэ нь дотоод сүлжээг ойлгомжгүй байдалд оруулж будлиан үүсгэдэг. Тиймээс энэ халдлагыг илрүүлэхдээ бродкаст хаяг руу ICMP пакет илгээгдэж байвал үүнийг халдлага хэмээн тодорхойлно.

IP-LAND халдлага нь хохирогч талын сүлжээг бусниулах зорилготой халдлага юм. Орж ирж буй пакетын гарсан хаяг нь тухайн халдлагад өртөж буй хостын хаягтай ижилхэн байдаг. Энэ үед тухайн хост орж буй халдлагын пакетуудын гарсан хаяг буюу өөрийнхөө хаяг руу хариу үзүүлж тухайн систем ойлгомжгүй байдалд ордог.

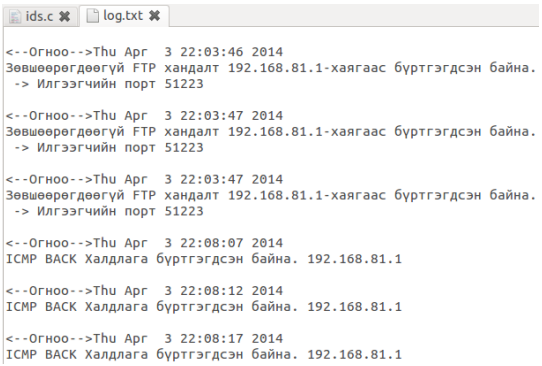
Системийг ажиллуулж эхлээд хамгийн эхэнд өөрийн шүүлт хийхийг хүсэж буй дүрмийг гараас бичиж оруулна. Ингэснээрээ та өөрийнхөө хүсэж буй урсгалыг хянаж чадах юм. Үүний давуу тал нь системийн илрүүлэлтийн хөдөлгүүрийн ачааллыг багасгаж, бүтээмжийг дээшлүүлэх юм.



Зураг 3. Халдлага илрүүлж буй байдал

Системийн илрүүлэлтийн хөдөлгүүр нь одоогоор тодорхой хэдэн тооны халдлагын сигнатур бүхий өгөгдлийн сантай бөгөөд үүнийхээ хүрээнд хангалттай сайн илрүүлэлт хийж байгаа юм.

Халдлага илрүүлэх системийн бас нэг салшгүй хэсэг бол халдлагын бүртгэл болох лог файл юм. Иймд, бид лог бичих функциональ боломжийг системдээ оруулж өгсөн бөгөөд илэрсэн халдлагыг огноо, цаг минуттай нь бүртгэж чадна. Үүний гол давуу тал нь аюултай хостыг илрүүлэх, цаашлаад мөрдлөг шалгалт хийх бололцоог олгох юм.



Зураг 4. Бичигдсэн лог файл

Дээрх зурагт илрүүлсэн халдлагын төрлийг болон халдагч этгээдийг IP хаяг болон портын дугаарыг лог файлд бичсэнийг харуулж байна.

VI. ДҮГНЭЛТ

Компьютерийн сүлжээний халдлага илрүүлэх систем нь болзошгүй халдлагад бэлтгэлтэй байж, ирж буй халдлага довтолгоог илрүүлдэг програм хангамж юм. Сүүлийн үед халдлагын тоо давтамж эрс өсөж буй нь халдлага илрүүлэх болон эсэргүүцэх системийн хэрэгцээ шаардлага эрс нэмэгдэж байна. Харамсалтай нь халдлага илрүүлэх системийн үнэ өртөг өндөр байдаг тул албан байгууллагууд тэр болгон энэ системийг худалдаж аваад байж чаддаггүй. Тиймээс болзошгүй халдлагын шинж чанарыг судлаж, түүнийг илрүүлэх болон эсэргүүцэх системийг хөгжүүлэх нь компьютерийн ухааны чиглэлээр судалгаа хийж буй хүмүүсийн хувьд чухал сэдэв юм.

Энэ судалгааны хүрээнд хөгжүүлсэн бүтээл маань ерөнхийдөө ХХИС юм. Манай систем нь өгөгдсөн дүрмийн хүрээнд хангалттай сайн ажилладаг. Цаашид уг системийг сэжигтэй пакетуудыг өгөгдлийн санд хадгалах болон системийн ажиллах хүрээг өргөжүүлэх зэргээр хөгжүүлэх шаардлагатай гэж үзэж байна.

АШИГЛАСАН МАТЕРИАЛ

[1] А. Ундармаа and Ч. Эрдэнэбат, “Өгөгдлийн сангийн програмын хамгаалалт,” in КТМС -ийн доктор, магистр оюутнуудын эрдэм шинжилгээний хурал, 2012, pp. 174–176.

[2] Н. Баатархуяг, “Мэдээллийн аюулгүй байдлын үндсэн зарчмууд,” in “Мэдээллийн аюулгүй байдал” онол, практикийн бага хурал, 2011.

[3] Мөнхбат, “Сүлжээний аюулгүй байдал ба хамгаалалт,” Munkhbat’s Weblog, 09-Oct-2007. [Online]. Available: http://munkhbat.wordpress.com/2007/10/09/hello-world/. [Accessed: 05-Apr-2014].

[4] С. Отгонлхагва, “Халдлага эсэргүүцэх систем,” МУИС, МТС, Улаанбаатар, 2009.

[5] Б. Бямбадорж, “Утасгүй сүлжээний халдлага илрүүлэх систем,” ШУТИС, КТМС, Улаанбаатар, 2013.

[6] “Home Page,” Snort. [Online]. Available: http://www.snort.org/. [Accessed: 05-Apr-2014].

[7] K. Dhangar, D. Kulhare, and A. Khan, “Intrusion Detection System (A Layered Based Approach for Finding Attacks),” Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 3, no. 5, pp. 277–283, 2013.

[8] R. C. Newman, Computer Security: Protecting Digital Resources. Jones & Bartlett Learning, 2009.

[9] “A Gentle Introduction to Haskell: Patterns,” Haskell, 1998. [Online]. Available: http://www.haskell.org/tutorial/patterns.html. [Accessed: 05-Apr-2014].

[10] S. K. Katsikas, “Intrusion Detection Systems.” University of Piraeus, 28-Jun-2010.

[11] J. Haas, “What is libpcap,” About.com. [Online]. Available: http://linux.about.com/cs/linux101/g/libpcap.htm. [Accessed: 05-Apr-2014].

[12] C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 4th ed. Prentice Hall, 2006, p. 880.

[13] “About,” Wireshark. [Online]. Available: http://www.wireshark.org/about.html. [Accessed: 18-Apr-2014].