Компьютерын Сүлжээний Өгөгдлийн Урсгалаас Халдлагийн Шинжилгээ

[1]Д.Бямбадорж, [2]Э.Мөнхцэцэг, [3]Б.Өсөхбаяр /PhD/, [3] Ж.Нямжав/проф PhD/
[1]Улаанбаатрын Их Сургууль, Физик электроникийн тэнхим
[2]Соёл-Эрдэнэ дээд сургууль
[3]Монгол Улсын Их Сургууль, Хэрэглээний Шинжлэх Ухаан Инженерчлэлийн сургууль
Электроник, Холбооны инженерчлэлийн тэнхим
Улаанбаатар хот, Монгол улс
pheelectro2013@gmail.com

***Хураангуй*— Энэхүү судалгааны ажилд Фэйспүүк болон Твиттер ээр дамжиж байгаа хөнөөлтэй пакет дээр анализ хийж, хөнөөл учруулах халдлага, дайралтыг илрүүлэхийн тулд Wireshark болон Zenmap програмын тусламжтайгаар дүн шинжилгээ хийж, шинээр гарч байгаа халдлагуудыг илрүүлэх болно. Туршилтын ажлыг виртул машин дээр дотоод сүлжээ нь tree топологиор холбогдсон 60 компьютерын сүлжээний өгөгдлийн урсгалыг менежменттэй свич ашиглан тухайн сүлжээгээр дамжиж байгаа өгөгдлийг Wireshark програмын тусламжтайгаар гурван сарын хугацаанд пакетуудыг цуглуулж дүн шинжилгээ хийсэн. Фэйспүүк болон Твиттер хандах үед тогтмол нэг IP хаяг болон сэжиг бүхий IP хаягуудыг www.virustotal.com сайтын тусламжтайгаар шалгаж үзэхэд хөнөөлтэй код агуулсан сайт болон вирустай болохыг тодорхойлсон. Тухайн сайт болон вирусыг нарийн судалж үзэхэд DoS төрлийн Neptune халдлага болохыг тодорхойлсон нь энэхүү өгүүллэгийн онцлог тал нь юм.**

Түлхүүр үг — Wireshark, DoS attack, SYN-Flood

I. УДИРТГАЛ

Мэдээлэл технологийн салбарт хурдацтай хөгжихийн хирээр мэдээлэлийн аюулгүй байдлыг хангах нь нэн тэргүүний асуудал болоод байна. Иймд мэдээлэлийг дамжуулж байгаа компьютерийн сүлжээний хамгаалат, хяналт зайлшгүй шаардлагатай бөгөөд антивирус, галт хана гэх мэт хамгаалалтын программ хангамжын тусламжтайгаар хамгаалах аргууд байдаг ч бүрэн дүүрэн хамгаалах боломжгүй. Тиймээс дотоод сүлжээний ачаалал дээр анализ хийснээр TCP давхаргын сүлжээний ачаалал нь олон тооны үүсгүүрүүдээс дамжигдаг юм. Халдалага илрүүлэх системийг сүлжээнд суурилсан болон хостод суурилсан гэж үндсэн хоёр хэсэгт хуваан авч үздэг бөгөөд сүлжээндэх халдлагыг илрүүлэхдээ сигнатюраар илрүүлэх болон гажилтаар илрүүлэх гэсэн үндсэн хоёр техникт тулгуурладаг.[1] Тодорхой нэг хэрэглэгч холболт хийхийн тулд TCP протоколыг ашиглан дамжуулалт хийхээс өмнө харилцах хоёр тал холболт тогтоосон байхыг шаарддаг. Холболт тогтоогоод дата дамжуулж дуусны дараа холболтыг салгадаг.TCP – ийн холболтыг “Three Way Handshake” буюу “Гурван- Болзолт Гар барилцах ” гэсэн аргаар тогтоодог. Man in the middle халдлага нь client болон server-лүү илгээж байгаа холболтын мэдээллийг дундаас нь олж авах зорлготой ба DoS –ийн төрлийн халдлага [10] хэрэглэгч интернэтэд холбогдох үед ихээхэн хэмжээний syn пакетийг илгээж TCP/IP ийн үйл ажиллагааг удаашруулдаг. Энэхүү судалгааны ажилд компьютерийн сүлжээгээр дамжиж байгаа пакет дээр анализ хийж, сүлжээний аюулгүй байдалд хор, хөнөөл учруулах халдлага, дайралтыг Wireshark [2] болон Zenmap[3-7] програмын тусламжтайгаар дүн шижилгээ хийж, шинээр гарч байгаа халдлагуудыг тодорхойлох юм.

II. СУДАЛГААНЫ АРГАЧЛАЛ

Компьютерийн дотоод сүлжээний шинжилгээг хийхэд тусгаарлагдсан тусгай хяналттай, тодорхой хамгаалалттай орчинг бүрдүүлэх шаардлагатай байдаг. Хяналттай тусгаарлагдсан орчинг бүрдүүлсний дараа үйдлийн системийн эхний төлөвийн мэдээллийг цуглуулж доорх програмуудыг хэрэглэн сүлжээний урсгал дээр анализ хийж гүйцэтгэдэг.

- ✓ Wireshark программ[2] нь пакет анализ хийгч бөгөөд сүлжээгээр дамжиж байгаа пакетыг барьж ямар протоколууд ямар өгөгдлийг зөөж байгааг харж болдог.
- ✓ Nmap программ[3-6] нь дотоод сүлжээний сул тал болон аюулгүй байдлыг шалгахад ашигладаг програм.
- ✓ RegShot программаар хостын регистрт өөрчлөлт орж байгаа эсэхийг нарийн тодорхойлох боломжтой.

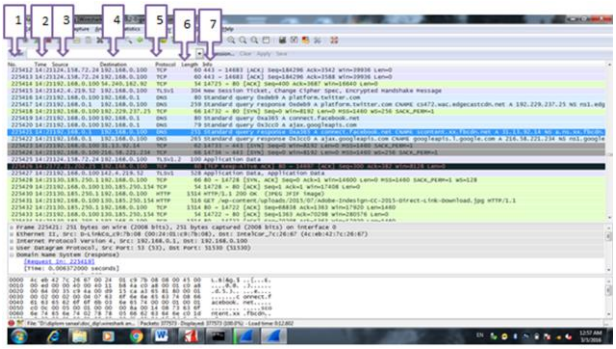
III. ТУРШИЛТ, ҮР ДҮН

Энэ ажлаар дотоод сүлжээний хэвийн болон халдлагатай пакет дээр дүн шинжилгээ хийсэн. Туршилтыг явуулахдаа I 7процессортай 4 гига рамтай компьютер дээр WMware програмыг ашиглан виртуал орчинд Windows 7 үйдлийн систем суулгаж үүсгэсэн. Виртуал орчинд үйдлийн системийн регистрийн мэдээллийг Regshot програмаар цуглуулсны дараа Дотоод сүлжээний төхөөрөмжүүдийн портын мэдээлэл сүлжээнд холбогдсон компьютерийн бүртгэлийг Zenmap програмын тусламжтай тодорхойлсон. Wireshark 2.0.1 програмыг ашилан сүлжээгээр дамжиж байгаа пакетуудыг цуглуулсан. Зураг 1-д үзүүлсэнээр Wireshark 2.0.1 програм дээр пакет цуглууж байгаа хэсэгийг харуулсан.

Энд:

1. No: Пакетыг дэс дараалалалд оруулах ашиглагдаг дугаар юм.
2. Time: Пакетыг барьж авсан үеийн он, сар , өдөр, цаг, минут секунтийг илэрхийлнэ.
3. Source: Пакет илгээсэн төхөөрөмжийн IP хаягыг харуулна.
4. Destination: Пакетын хүлээн авах төхөөрөмжийн IP хаягыг харуулна.
5. Protocol: Барьж авсан пакетын протоколын төрлийг харуулна.
6. Length: Пактын хэмжээг харуулна.
7. Info: Пакетын тухай нэмэлт мэдээлэл харуулна.

Томъёо 1 дагуу цэгэн гэрэл үүсгэгч бүхий дэлгэцийн аргаар элементар дүрс үүсгэхдээ хүснэгт 1-д үзүүлсэн параметрүүдийн дагуу бодсон.



Зураг 1. Wireshark програрамаар цуглуулсан пакет

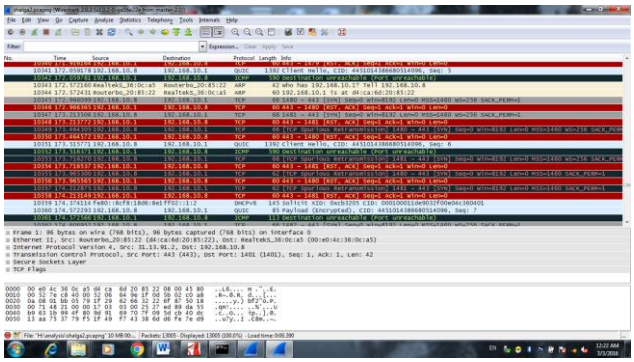
Wireshark программаар сүлжээний өгөгдлийн урсгалаас халдлагыг илрүүлэхдээ дотоод сүлжээний рүүтер эсвэл хостын түвшний пакетуудын мэдээлэл дээр тулгуурлан сэжигтэй пакетуудын дата дамжуулалт болон хүлээн авсан протокол дээр анализ хийсний үр дүнд IP 31.13.92.14 хаягийг тодорхойлсон. Уг IP 31.13.92.14 хаягийг www.virustotal.com сайтад upload хийснээр дараах үр дүн гарсан. Үүнд:

- Phishing сайтуудтай

  xx.fbcdn.net
  - a.ns.xy.fbcdn.net
  - a.ns.t.fbcdn.net
  - a.ns.fna.fbcdn.net
  - a.ns.t.tfbnw.net

  Adware.Downware.9804 (вирус)
  HEUR:Trojan.Win32.Generic (вирус) дээрх xx.fbcdn.net сайт болон вирус нь хохирогч компьютерлуу халдах боломжтойг www.virustotal.com сайтаар тодорхойлсон.

IP 31.13.92.14 хаягийг нарийн судалахын тулд www.facebook.com – ийн шинэ хэрэглэгч нээж, xx.fbcdn.net хаягийг сонгон авч, виртуал машины тусламжтай ачааллаж хост болон дотоод сүлжээнд хэрхэн



Зураг 2. Халдлагад өртсөн үеийн пакет.

нөлөөлж байгааг Regshot болон Wireshark программын тусламжтай дүн шинжилгээ хийсэнийг зураг 2-д үзүүлсэн.

Зураг 2-ийн үр дүнд Denial of Service төрлийн Neptune халдлага болохыг тодорхойлсон. Уг халдлага нь TCP/IP аар их хэмжээний SYN пакетыг 443 портоор илгээж хостын үйл ажиллагааг удаашруулж системд гажуудал үүсгэж интернэт холболт тасалдаж байгаа нь харагдаж байна.

Физик машин дээр суурилсан виртуал үйдлийн системийн регистрийн мэдээллийг урьдчилан Regshot программаар цуглуулсны дараах халдварлагдаагүй болон халдварлагдсан үеийн регистртэй харьцуулсан мэдээлэл дээр дүн шинжилгээ хийсэн бөгөөд хостын регистрд хэрхэн өөрчлөлт орсныг хүсгнэгт №1 үзүүлэв.

ХҮСНЭГТ 1. РЕГИСТРД ӨӨРЧЛӨЛТ ОРУУЛСАН ХЭСГҮҮД.

Windows registry	DoS attack
HKLM\Software\Microsoft	
HKLM\System\ControlSet001\Control\	
HKLM\Hardware\	
HKLM\System\CurrentControlset\Services\	
HKLM\Software\Microsoft\Cryptography\	
HKLM\Software\Microsoft\Windows NT\CurrentVersion\	
HKU\S-1-5-21-602162358-492894223-299502267-500\Software\Microsoft\Windows\CurrentVersion\Run	**X**
HKLM\SOFTWARE\Microsoft\Direct Draw\MostRecentApplication	

HKEY_USERS бүртгэл нь (HKU) HKEY_CURRENT_USER товчлол бөгөөд тухайн хэсэгт Виндоус үйдлийн системд байгаа бүх хэрэглэгчдийн үндсэн тохиргоо мэдээлэл хадгаладсан байдаг [11-12] бөгөөд энэ регистр нь халдалгат өртсөнөөр хэрэглэгчдийн үндсэн тохиргоонд өөрчлөлт оруулдаг.

IV. ДҮГНЭЛТ

Бид судалгааны ажлын хүрээнд УБИС, МҮИС, СЭДС сургуулуудын компьютерийн дотоод сүлжээний урсгал дээр анализ хийсэн ба Wireshark програмын тусламжтай түгээмэл ашигладаг www.facebook.com болон www.twitter.com -ээр тархсан халдлагыг илрүүлэхийг зорьсон. Дээрх судалгааны үр дүнд халдварлуулсан www.facebook.com хаягийг ашиглан дүн шинжилгээ хийсэн. Туршилтын үр дүнд DoS төрлийн Neptune халдлагыг тодорхойлсон. Neptune халдлага нь хостын үйл ажиллагаа болон интернэт холболтыг тасалдуулах зорилготой болох нь дээрх туршилтын үр дүнгээс харадаж байна. Цаашид энэхүү судалгааны ажлыг DDoS төрлийн халдлагатай харьцуулан нарийвчилан судлах зорилготой.

АШИГЛАСАН МАТЕРИАЛ

[1] Robert Mitchell, Ing-Ray Chen, A survey of intrusion detection techniques for cyber-physical systems, April 2014, ACM Computing Surveys Volume 46 Issue 4

[2] “About,” Wireshark. [Online]. Available: http://www.wireshark.org/about.html. [Accessed: 18-Apr-2014]The History and Future of Nmap. Nmap.org. Retrieved on 2013-02-01.

[3] The History and Future of Nmap. nmap.org. Retrieved 2008-05-14.

[4] "Matrix mixes life and hacking". BBC News. 2003-05-19. Retrieved 2009-01-14.

[5] Nmap Scripting Engine. Nmap.org. Retrieved on 2013-02-01

[6] Tanenbaum, Andrew S. (2003-03-17). Computer Networks (Fourth ed.). Prentice Hall.ISBN 0-13-066102-3.

[7] http://en.wikipedia.org/wiki/Windows_Registry

[8] http://kb.chemtable.com/ru/windows-registry-main-keys.htm#hkcu

[9] https://en.wikipedia.org/wiki/Man-in-the-middle_attack