ҒТАМР 20.15.05 https://doi.org/10.58805/kazutb.v.2.23-297

ЖЕЛІ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУДЕ ТРАФИКТІ ТАЛДАУ ҚҰРАЛДАРЫН ҚОЛДАНУ АРҚЫЛЫ АУЫТҚУЛАР МЕН ЫҚТИМАЛ ҚАУІПТЕРДІ АНЫҚТАУ

Ж. Бидахмет, А. Уайда✉, Р.Е.Әлішер, Д. Бағдаулет, Қ. Қаржаубаев , А.Сердалы, Ә. Ахметов

әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан,

e-mail: uaida_a@mail.ru

Мақалада компьютерлік желілерде ақпарат жинау әдістері және олардың қазіргі цифрлық қоғамдағы желілік қауіпсіздікті қамтамасыз етудегі маңызы қарастырылады, яғни компьютерлік желілердегі ақпаратты түсіру құралдарының желілік қауіпсіздігі талданады. Қазіргі ақпараттық қоғамда бұл құралдардың маңызы артып келеді. Трафикті талдау процесі желі арқылы берілетін деректерді бақылау, жазу және талдау арқылы ауытқулар мен ықтимал қауіптерді анықтауды қамтиды. Мақалада Wireshark, Tcpdump және Macof сияқты құралдардың функционалдығы мен қолдану әдістері тереңірек қарастырылған. Осы құралдарды қолдану әдістері талқыланып, олардың әрқайсысының ерекшеліктері мен мүмкіндіктері көрсетілген. Әртүрлі желілік құралдарды тиімді пайдалану арқылы желідегі қауіп-қатерлерді алдын-ала анықтау және жою мүмкіндігіне баса назар аударылды. Бұл құралдардың көмегімен желілік қауіпсіздік деңгейін арттыруға, желі ақауларын жылдам табуға және жоюға болатыны көрсетілген. Сонымен қатар, мақалада әрбір құралдың артықшылықтары мен кемшіліктерін салыстыра отырып, олардың қай жағдайда тиімді екені анықталды.

Түйін сөздер: ақпарат, желі, қауіпсіздік, трафик, Wireshark, Tcpdump, Macof

ВЫЯВЛЕНИЕ ОТКЛОНЕНИЙ И ПОТЕНЦИАЛЬНЫХ УГРОЗ С ПОМОЩЬЮ ИНСТРУМЕНТОВ АНАЛИЗА ТРАФИКА В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ СЕТИ

Ж. Бидахмет, А. Уайда✉, Р.Е. Алишер, Д. Багдаулет, К. Каржаубаев, А.Сердалы, А. Ахметов

Казахский национальный университет им. Аль-Фараби, Алматы, Казахстан,

e-mail: uaida_a@mail.ru

В статье рассматриваются методы сбора информации в компьютерных сетях и их значение для обеспечения сетевой безопасности в современном цифровом обществе, т. е. анализируется сетевая безопасность средств захвата информации в компьютерных сетях. В современном информационном обществе значение этих средств возрастает. Процесс анализа трафика включает выявление аномалий и потенциальных угроз путем мониторинга, записи и анализа данных, передаваемых по сети. В статье подробно рассматриваются функциональные возможности и методы использования таких инструментов, как Wireshark, Tcpdump и Macof. Обсуждаются методы применения этих средств, демонстрируются особенности и возможности каждого из них. Упор был сделан на возможность заранее выявлять и устранять угрозы в сети с помощью эффективного использования различных сетевых инструментов. Было показано, что с помощью этих инструментов можно повысить уровень сетевой безопасности, быстро найти и устранить проблемы с сетью. Кроме того, в статье сравниваются преимущества и недостатки каждого средства, чтобы определить, в каких случаях они наиболее эффективны.

Ключевые слова: информация, сеть, безопасность, трафик, Wireshark, Tcpdump, Macof

IDENTIFY DEVIATIONS AND POTENTIAL THREATS USING TRAFFIC ANALYSIS TOOLS TO ENSURE NETWORK SECURITY

Zh.Bidakhmet, A. Uaida✉, Alisher R., D. Bagdaulet, K. Karzhaubaev, A. Serdaly, A. Akhmetov

Al-Farabi Kazakh National University, Almaty, Kazakhstan,

e-mail: uaida_a@mail.ru

The article discusses methods of information capture in computer networks and their importance for network security in today's digital society, i.e. it analyzes the network security of information capture tools in computer networks. In today's information society, the importance of these tools is increasing. The process of traffic analysis involves identifying anomalies and potential threats by monitoring, recording and analyzing data transmitted over the network. The article discusses in detail the functionality and methods of using tools such as Wireshark, Tcpdump and Macof. The methods of using these tools are discussed, the features and capabilities of each of them are demonstrated. The emphasis was placed on the ability to identify and eliminate threats in the network in advance through the effective use of various network tools. It has been shown that using these tools it is possible to increase the level of network security, quickly find and fix network problems. In addition, the article compares the advantages and disadvantages of each remedy to determine in which cases they are most effective.

Keywords: information, network, security, traffic, Wireshark, Tcpdump, Macof

Кіріспе. Қазіргі ақпараттық қоғамда деректерді тасымалдау әртүрлі желелік орталарда жүзеге асырылады. Сондықтан деректерді тасымалдау қауіпсіздігін қамтамасыз ету және құпия ақпаратты қорғау басты мәселе болып табылады. Бұл контексте негізгі аспектілердің бірі ақпаратты ұстау құралдарын талдау болып табылады.

Деректерді ұстап алу - бұл желі арқылы берілетін немесе электронды түрде сақталған деректерді заңсыз немесе рұқсат етілген жинау процесі. Бұл процесс желілік трафикті бақылауды, хабар мазмұнын талдауды және сақтау құрылғыларынан деректерді жинауды қамтуы мүмкін [1].

Желі қауіпсіздігін қамтамасыз етуде трафикті талдау басты рөл атқарады. Ол желілік инфрақұрылымға бағытталған ықтимал қауіптерді, ауытқуларды және шабуылдарды анықтауға мүмкіндік береді. Деректердің тасымалдануын бақылау және пакеттерді талдау арқылы оқиғаларға тез жауап беруге және құпия ақпараттың ағып кетуіне жол бермеуге болады [2].

Трафикті талдау желілік инфрақұрылымның осалдықтарын анықтауға және жоюға мүмкіндік береді, оның әртүрлі шабуыл түрлерінен сенімді қорғалуын қамтамасыз етеді. Бұл процесс сонымен қатар желі өнімділігін жақсарту мүмкіндіктерін анықтау арқылы желі өнімділігін оңтайландыруға көмектеседі. Тыңдауды талдау желі қауіпсіздігін қамтамасыз ету және деректердің құпиялылығын қорғаудың маңызды құралы болып табылады. Төменде біз осы процестің негізгі аспектілерін, трафикті талдау әдістерін және осы салада тиімді жұмыс істеу үшін қолданылатын құралдарды қарастырамыз.

Материалдар мен әдістер. Желілік трафикті талдау құралдары – компьютерлік желілерде деректердің берілуін бақылауға көмектесетін бағдарламалар мен утилиталар. Олар желі арқылы өтетін ақпаратты көруге, талдауға және жазуға мүмкіндік береді. Бұл құралдар желі проблемаларын анықтауға ғана емес, сонымен қатар деректерді беру қауіпсіздігін қамтамасыз етуге және желілік трафиктегі ықтимал қауіптер мен ауытқуларды анықтауға көмектеседі. Бұл мәселелерді тиімді шешу үшін желілік трафикті талдаудың бірнеше қуатты құралдары бар, олардың арасында Wireshark, Tcpdump және Macof ерекшеленеді [3].

Wireshark – желі белсенділігін бақылауға, талдауға және жөндеуге мүмкіндік беретін қуатты желі трафигін талдау құралы. Ол желілік интерфейс арқылы өтетін деректер пакеттерін ұстап алуға және әрбір пакет туралы егжей-тегжейлі ақпаратты, соның ішінде протокол тақырыптарын, деректер мен басқа сипаттамаларды беруге қабілетті.

Wireshark негізгі мүмкіндіктері мен мүмкіндіктеріне мыналар жатады:

1. Қолдау көрсетілетін бірнеше протоколдар: Wireshark 2000-нан астам әртүрлі желілік протоколдарды қолдайды, бұл оны әртүрлі желі сценарийлерін талдауға арналған әмбебап құрал етеді.
2. Графикалық пайдаланушы интерфейсі (GUI): Қарапайым және интуитивті интерфейс Wiresharkпен жұмыс істеуді тәжірибелі және жаңадан ба-

стаған пайдаланушылар үшін ыңғайлы етеді.

3. Сүзу және іздеу: үлкен көлемдегі деректерді өңдеуді жеңілдете отырып, тек қажетті ақпаратты бөлектеуге және талдауға мүмкіндік береді.

Wireshark - желі әкімшілері, қауіпсіздік инженерлері, желілік қосымшаларды әзірлеушілер және желілік инфрақұрылыммен жұмыс істейтін кез келген басқа адамдар үшін маңызды құрал.

Tcpdump – желілік трафикті талдауға арналған пәрмен жолы утилитасы. Ол компьютердің желілік интерфейсі арқылы өтетін деректер пакеттерін ұстауға және көрсетуге мүмкіндік береді. Tcpdump бағдарламасының маңызды ерекшелігі оның нақты уақыт режимінде жұмыс істеу мүмкіндігі болып табылады, бұл оны желі мәселелерін диагностикалау және талдау үшін қуатты құрал етеді [4].

Tcpdump негізгі мүмкіндіктері мен функцияларына мыналар жатады:

1. Көп протоколды қолдау: Tcpdump TCP, UDP, ICMP және т.б. сияқты әртүрлі желілік протоколдарды пайдаланып пакеттерді талдауға қабілетті.
2. Трафикті сүзу: пайдаланушыға тек белгілі бір пакеттерді (мысалы, дереккөз, тағайындалған орын, порт және басқа параметрлер бойынша) көрсету үшін нақты критерийлерді көрсетуге мүмкіндік береді.
3. Файлдарды оқу және жазуды қолдау: Tcpdump желі трафигінің сақталған файлдарымен жұмыс істей алады, сонымен қатар кейінірек талдау үшін файлға ағымдағы трафикті жаза алады.

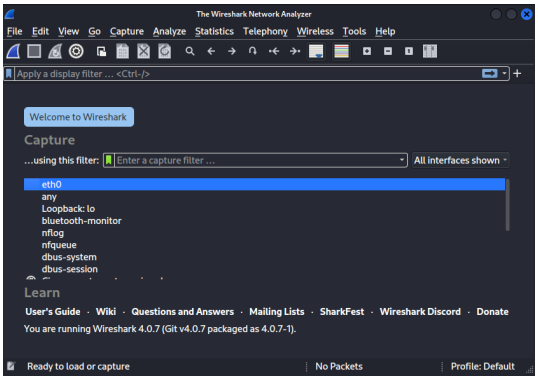
Tcpdump – желі әкімшілері, қауіпсіздік инженерлері және желілік трафикті талдаумен жұмыс істейтін кез келген адам үшін маңызды құрал.

Macof - бұл кездейсоқ MAC мекенжайларының үлкен санын жасауға және оларды желіге жіберуге арналған пәрмен жолы құралы. Macof бағдарламасының негізгі мақсаты - желі жұмысын баяулату немесе бұзу үшін жалған MAC мекенжайларының көп санын жасау [5].

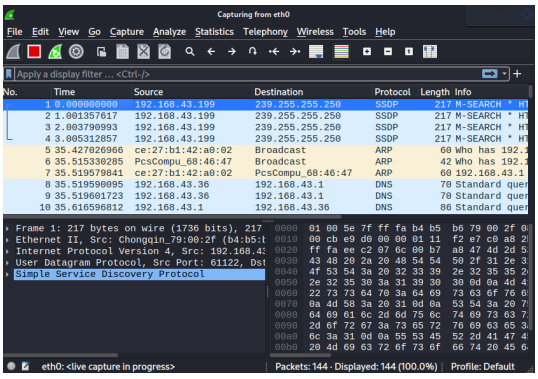
Macof көмегімен жалған MAC мекенжайларын жасау мүмкіндіктері мыналарды қамтиды:

1. Кездейсоқ генерация: Macof MAC мекенжайларын кездейсоқ түрде жасайды, бұл оларды болжауды қиындатады.
2. Желіге жіберу: Жасалған MAC мекенжайлары компьютердің желілік интерфейсі арқылы желіге жіберіледі.
3. Ықтимал шабуылдар: Macof коммутаторлар сияқты желілік құрылғыларды шамадан тыс жүктеуге немесе баяулатуға бағытталған шабуылдарда қолданылуы мүмкін.

Macof пайдалану сақтықты қажет ететінін ескеру маңызды, себебі бұл құралды дұрыс пайдаланбау желінің бұзылуына және қажетсіз жүктемеге әкелуі мүмкін. Ол көбінесе желілік қауіпсіздікті тестілеуде және желіні оқытуда қолданылады.



1-сурет - Интерфейсті таңдау



2-сурет -Жиналған пакеттер

Нәтижелер мен талқылау. Wireshark мысалы: Енді біз Wireshark трафикті ұстау және талдау мүмкіндіктерін көрсетеміз. Wireshark-ты іске қосып, тізімнен бақылау интерфейсін таңдайық, біздің жағдайда бұл eth0 болады (1-сурет).

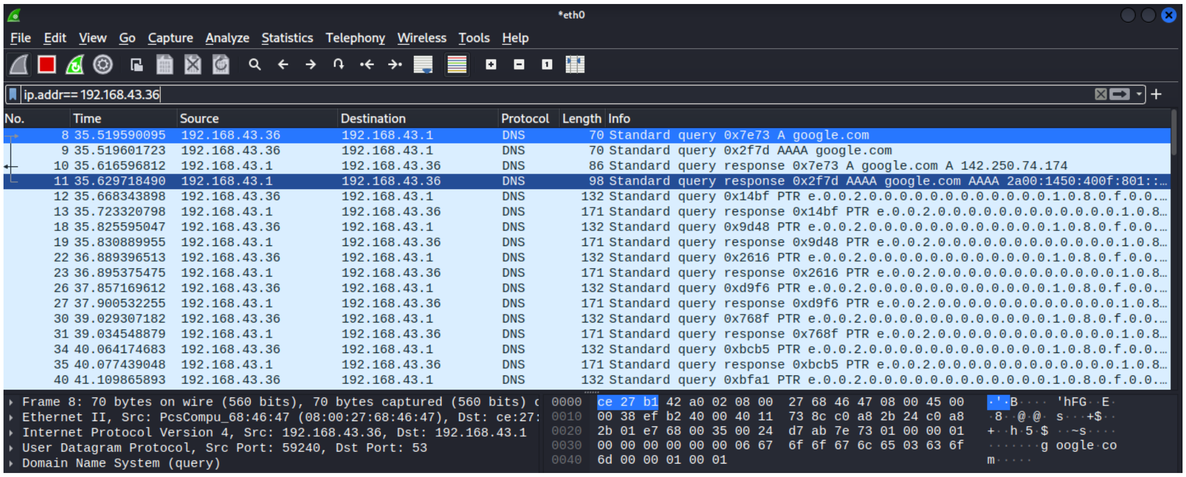
Интерфейсті таңдағаннан кейін деректерді жинау басталады. Тараудың басында біз сымсыз желілердегі трафикті бақылау өте қарапайым екенін айттық. Міне осылай - сымсыз желідегі барлық компьютерлерден деректерді көру үшін сізге қажетті интерфейсті таңдау керек.

Қажетті деректер көлемін жинағаннан кейін па-

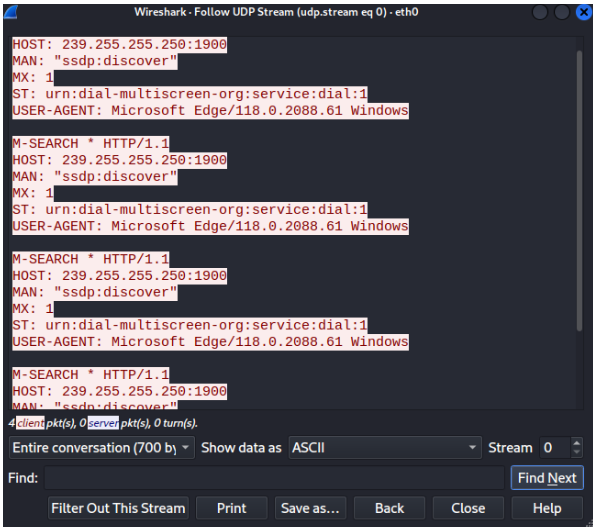
кеттерді жинауды тоқтатыңыз (2-сурет). Енді оларды кейінірек талдау үшін сақтауға немесе оны бірден бастауға болады. Бірнеше минут ішінде біз 20 000-ға жуық пакет жинадық, бұл желідегі трафик аз болған жағдайда болды. Әрине, мұндай пакеттерді қолмен қарау өте көп еңбекті қажет ететін жұмыс және оны жеңілдету үшін Wireshark әртүрлі сүзгілерді ұсынады (1-кесте).

1-кесте - Wireshark сүзгілері

Оператор	Функция	Мысал
==	Тең	Ip.addr == 192.168.10.12
eq	Тең	Tcp.port eq 80
!=	Тең емес	Ip.addr != 192.168.10.5
ne	Тең емес	Ip.src ne 192.168.10.5
contains	Құрамында	Hhtp contains “google.com”



3-сурет- Веб-сервермен байланыс



5-сурет- Барлық пайдалы ақпарат бір жерде

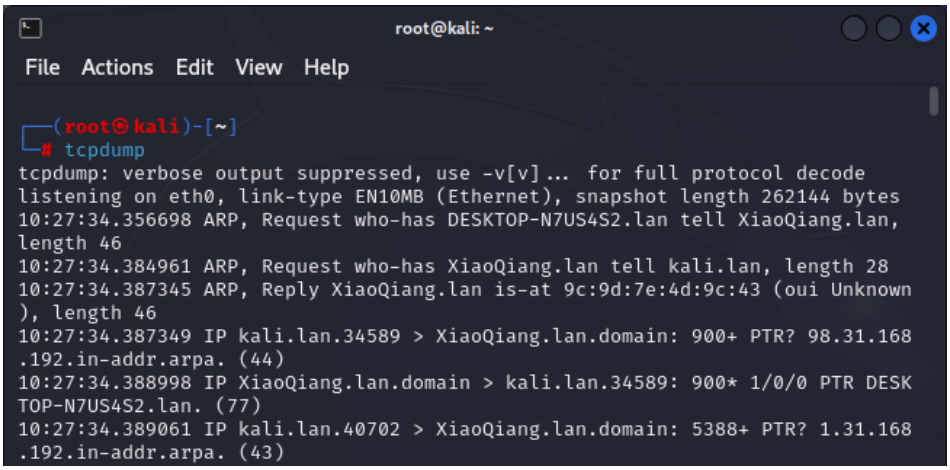
Google.com веб-сайтына пайдаланушы сұрауларын сүзгіден өткізейік. DNS сұрауынан бастайық, өйткені ол әрқашан бірінші болады. Сүзгіні қолдану арқылы біз браузер сұрауларының және DNS серверіне жауаптардың толық, дәйекті тарихын көреміз. Енді қай IP мекенжайы әрі қарай байланыс болатынын біле отырып, сәйкес сүзгіні жасайық (ip.addr==192.168.43.36) (3-сурет).

Көріп отырғаныңыздай, сүзгіден өткен пакеттердің саны 1153 (3-сурет). Олардың әрқайсысы деректердің аз ғана бөлігін ғана жібереді және олардағы қандай ақпарат бар екенін түсіну өте қиын. Тапсырманы жеңілдету үшін Wireshark нақты деректер ағынын бақылаудың керемет мүмкіндігіне ие. UDP жағдайында «UDP Stream» опциясын таңдаңыз [6].

Сонымен, біз байланыстың толық, стандартты бейнесін көрдік - DNS серверінен сұраныс пен жауап, үш жақты қол алысу және деректерді беруді инициализациялау. Оның үстіне біз пакеттердің мазмұнын да көрдік (5-сурет).

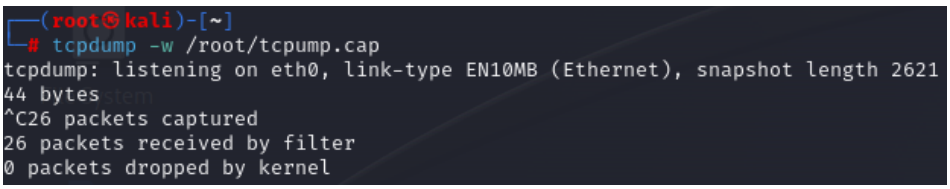
Графикалық интерфейске әрқашан қол жеткізе алмайтыныңызды ескеріңіз, сондықтан Wireshark алдында пайда болған басқа құрал - tcpdump-пен танысуды ұсынамыз.

Tcpdump мысалы: Егер сіз жай ғана tcpdump іске қоссаңыз, онда барлық ақпарат нақты уақыт режимінде шығарылады, бұл кейіннен оны талдау үшін іс жүзінде жарамсыз етеді (6-сурет).



6-сурет - Tcpdump командасының нәтижесі

Барлық ақпаратты файлға сақтау әлдеқайда жақсы, өйткені бұл деректерді жинауды жеңілдетеді және сізге ыңғайлы кез келген уақытта кейінгі трафикті талдау мүмкіндігін жасайды (7-сурет).



7-сурет- Ақпаратты tcpump.cap парақшасына сақтаймыз

Алынған деректерді талдау үшін консольді пайдалануға болады. Біз дәйекті боламыз және консольдегі деректерді талдауға мысал келтіреміз.

Қосылым болған барлық IP мекенжайлары мен порттарын қарастырайық (8-сурет):

```
┌──(root㉿kali)-[~]
└─# tcpdump -n -r /root/tcpump.cap | awk -F" " '{print $3}' | sort -u | head
reading from file /root/tcpump.cap, link-type EN10MB (Ethernet), snapshot len
gth 262144
192.168.31.112.54832
192.168.31.112.54833
192.168.31.98.5353
192.168.31.98.61162
192.168.31.98.61164
Reply
Request
fe80::3135:7a21:9f94:e307.5353
```

8-сурет - Қосылған IP мекенжайлар тізімі

Әрі қарай, оны түсіру кезінде желі арқылы жіберілген ақпаратты қарастырайық. Бұл жағдайда біз оны HEX форматында көреміз, бірақ бұл бізге қажетті деректерді алуға кедергі болмайды (9-сурет).

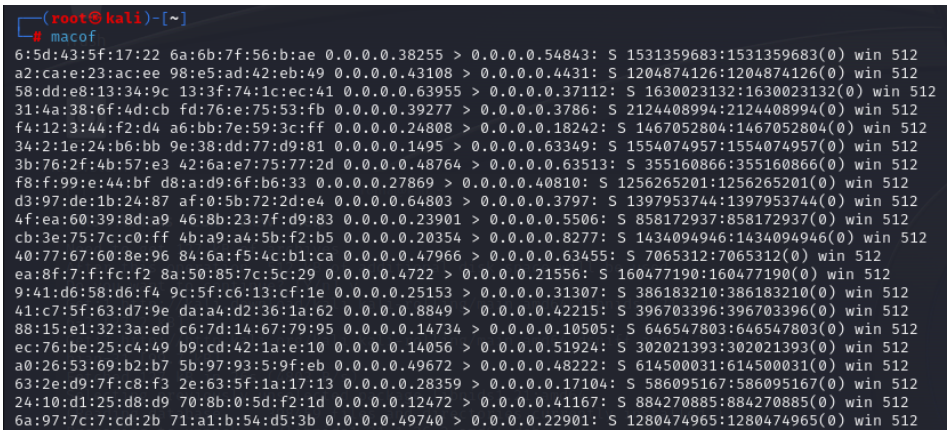
```
┌──(root㉿kali)-[~]
└─# tcpdump -nX -r /root/tcpump.cap
reading from file /root/tcpump.cap, link-type EN10MB (Ethernet), snapshot len
gth 262144
10:31:16.291196 ARP, Request who-has 192.168.31.98 tell 192.168.31.1, length
46
        0×0000:  0001 0800 0604 0001 9c9d 7e4d 9c43 c0a8  ..........~M.C..
        0×0010:  1f01 0000 0000 0000 c0a8 1f62 0000 0000  ...........b....
        0×0020:  0000 0000 0000 0000 0000 0000 0000       ..............
10:31:34.817663 IP 192.168.31.98.61162 > 239.255.255.250.1900: UDP, length 17
5
        0×0000:  4500 00cb 129b 0000 0111 d682 c0a8 1f62  E..............b
        0×0010:  efff fffa eeea 076c 00b7 b484 4d2d 5345  .......l....M-SE
        0×0020:  4152 4348 202a 2048 5454 502f 312e 310d  ARCH.*.HTTP/1.1.
        0×0030:  0a48 4f53 543a 2032 3339 2e32 3535 2e32  .HOST:.239.255.2
        0×0040:  3535 2e32 3530 3a31 3930 300d 0a4d 414e  55.250:1900..MAN
        0×0050:  3a20 2273 7364 703a 6469 7363 6f76 6572  :."ssdp:discover
        0×0060:  220d 0a4d 583a 2031 0d0a 5354 3a20 7572  "..MX:.1..ST:.ur
        0×0070:  6e3a 6469 616c 2d6d 756c 7469 7363 7265  n:dial-multiscre
        0×0080:  656e 2d6f 7267 3a73 6572 7669 6365 3a64  en-org:service:d
        0×0090:  6961 6c3a 310d 0a55 5345 522d 4147 454e  ial:1..USER-AGEN
        0×00a0:  543a 204d 6963 726f 736f 6674 2045 6467  T:.Microsoft.Edg
        0×00b0:  652f 3131 382e 302e 3230 3838 2e36 3120  e/118.0.2088.61.
        0×00c0:  5769 6e64 6f77 730d 0a0d 0a              Windows....
10:31:35.819020 IP 192.168.31.98.61162 > 239.255.255.250.1900: UDP, length 17
5
```

9-сурет -Жіберілген ақпараттар HEX-форматында

Енді шабуылдаушы коммутатор порттарының біріне қол жеткізе алатын жағдайды қарастырайық. Бұл жағдайда коммутатордың өзіне қол жеткізу немесе оның басқа бөлмеде орналасқан желілік жабдыққа қосылған желілік розетка екендігі маңызды емес. Жалғыз маңызды нәрсе - желілік интерфейс тек келуі керек пакеттерді қабылдайды, одан артық емес.

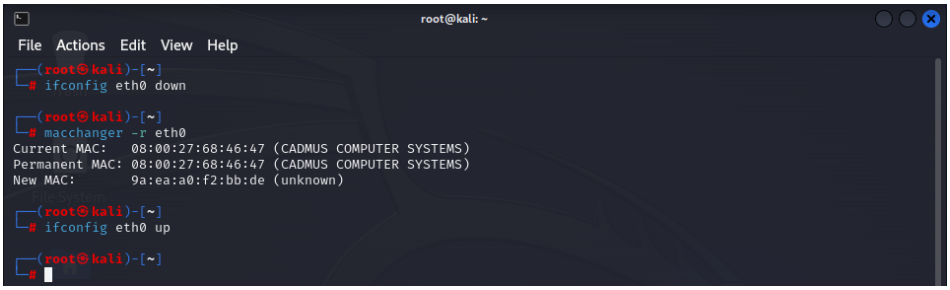
Мұндай қорғанысты айналып өтудің және коммутаторды хаб ретінде жұмыс істеуге мәжбүрлеудің ең танымал тәсілдерінің бірі, бұл бізге барлық желілік трафикті тоқтатуға мүмкіндік береді, CAM кестесін толтыру болып табылады [7-8].

CAM кестесін MAC мекенжайларымен толтыруға бағытталған шабуылды орындау үшін бір пәрмен жеткілікті (10-сурет):



10-сурет - Macof шабуылы

Тағы бір айта кететін мәселе бар. Егер сіз желілік порттардың біріне қол жеткізсеңіз де, сіз әлі де желіге кіре алмайсыз, өйткені барлық заманауи коммутаторлар MAC мекенжайлары бойынша қол жеткізуді басқара алады. Дегенмен, сізде әрқашан компьютердің MAC мекенжайын келесідей өзгерту мүмкіндігі бар (11-сурет):



11-сурет - MAC мекенжайына өзгертулер

Трафик талдауы желі өнімділігі туралы құнды түсінік береді және қауіпсіздік үшін маңызды болуы мүмкін. Дегенмен, оны өткізу кезінде этикалық нормаларды сақтауды ұмытпаған жөн. Пайдаланушы деректерінің құпиялылығы мен құпиялылығын ескеру қажет. Жол қозғалысын талдау нәтижесінде алынған ақпаратты жинау, талдау және сақтау кезінде деректерді қорғаудың барлық заңдары мен саясаттарын сақтау ұсынылады.

Деректерді қорғаудың криптографиялық әдістерінің дамуымен шифрланған трафикті талдау барған сайын қиындай түсуде. Шифрлау пакет мазмұнын егжей-тегжейлі талдауға елеулі кедергі келтіруі мүмкін. Сарапшылар шифрланған трафикпен жұмыс істеу дағдыларын дамытуы және шифрланған байланыстағы қауіптерді анықтай және талдай алатын талдау әдістерін іздеуі керек [9].

Бұл аспектілер трафикті талдаумен жұмыс істеу кезінде аналитиктер кездесетін шектеулер мен қиындықтарды түсіну үшін маңызды. Осы факторларды ескере отырып, сарапшылар анағұрлым тиімді талдау стратегиялары мен әдістерін жасай алады. Технологияның дамуымен және желілік трафиктің жаңа түрлерінің пайда болуымен оны талдаудың инновациялық тәсілдерінің қажеттілігі туралы сұрақ туындайды. Желінің қауіпсіздігі және трафикті талдау саласындағы жетекші сарапшылар қауіптерді тиімдірек анықтап, талдай алатын жаңа әдістер мен алгоритмдерді құрумен айналысуда. Трафикті талдау саласында жасанды интеллект, машиналық оқыту және үлкен деректерді талдауды пайдалану перспективалы бағыт болып табылады [10].

Басқа қауіпсіздік құралдарымен интеграция. Желінің тиімді қауіпсіздігі кешенді тәсілді қажет

етеді. Трафикті талдауды басқа қауіпсіздік құралдарымен, мысалы, қауіпті бақылау жүйелерімен, шабуылды анықтау құралдарымен және DDoS қорғау жүйелерімен біріктіру желілік инфрақұрылымды қорғаудың сенімді және тиімді тетіктерін жасауға мүмкіндік береді [11].

Қорытынды. Зерттеуде желілік трафикті талдаудың негізгі аспектілері, соның ішінде қолданылатын құралдар, талдау әдістері, сондай-ақ осы саланың дамуындағы шектеулер мен перспективалар қарастырылды. Wireshark, Tcpdump және Macof сияқты маңызды құралдардың мүмкіндіктері мен қолданбалары талқыланды. Желілік трафикті талдаудың әртүрлі аспектілері, соның ішінде аномалияларды анықтау, желі өнімділігін бақылау және қауіпсіздік инциденттерін зерттеу әдістері қарастырылды.

Желілік трафикті талдау құралдарын пайдалану желі қауіпсіздігін қамтамасыз етудің маңызды элементі болып табылады. Бұл құралдар аномалияларды анықтап, қауіптерді тауып, желінің жағдайын бақылап, қауіпсіздік инциденттеріне жауап беруге мүмкіндік береді. Трафикті талдау арқылы мамандар қауіптерге жылдам жауап беріп, шабуылдардың алдын алып, желілік инфрақұрылымның үздіксіз жұмысын қамтамасыз етеді.

Желілік трафикті талдау құралдарын пайдалану желінің қауіпсіздік деңгейін айтарлықтай арттырып, өзгермелі жағдайлар мен қауіптерге жылдам әрекет етуге мүмкіндік береді. Трафикті талдаудың заманауи әдістерін әзірлеу және енгізу, оны басқа қауіпсіздік құралдарымен біріктіру және осы саладағы өзгерістерді үздіксіз бақылау желілік инфрақұрылымның қауіпсіздігін қамтамасыз етудегі маңызды қадамдар болып табылады.

Әдебиеттер

1.Chris Sanders Practical Packet Analysis, 3rd Edition: Using Wireshark to Solve Real-World Network Problems 3rd Edition// No Starch Press. -2017.- P.120-145, 2017. ISBN: 978-1593278021

2. Chris Sanders, Jason Smith Applied Network Security Monitoring: Collection, Detection, and Analysis 1st Edition// Syngress.-2013.- P.200-210. ISBN 978-0124172081.

3.Michael Sikorski, Andrew Honig Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software 1st Edition// No Starch Press.-2012.-P.325. ISBN: 978-1593272906

4. Sherri Davidoff, Jonathan Ham Network Forensics: Tracking Hackers through Cyberspace 1st Edition.//Prentice Hall. -2012.-576 P. ISBN 978-0132564717

5. Laura Chappell Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide 2nd Revised ed. Edition// University Laura Chappell.-2012.- P.250-256. ISBN 978-1893939943

6. Richard Stevens TCP/IP Illustrated: The Protocols, Volume 1 (Addison-Wesley Professional Computing Series) 2nd Edition.-2011.-P. 65-75. ISBN: 978-0321336316.

7. William Stallings Network Security Essentials: Applications and Standards 6th Edition.-2016.- P.290-302.ISBN: 978-0134527338

8.A. Rahmatulloh, R. Gunawan, and F. M. S. Nursuwars Performance comparison of signed algorithms on JSON Web Token //in IOP Conference Series: Materials Science and Engineering.- 2019.- Vol.550(1):012023. DOI 10.1088/1757-899X/550/1/012023

9. A. Neumann, N. Laranjeiro, J. Bernardino An Analysis of Public REST Web Service APIs //IEEE Trans Serv Comput.- 2021.- Vol. 14(4).- P.957-970. DOI 10.1109/TSC.2018.2847344.

10. G. Alonso, F. Casati, H. Kuno, V. Machiraju. Web Services// in Web Services: Concepts, Architectures and Applications- Eds. Berlin, Heidelberg: Springer Berlin Heidelberg.- 2004.- P. 123-149. DOI 10.1007/978-3-662-10876-5_5.

11.Бидахмет Ж.,Уайда А., Майлыбаева А.Д., Даркенбаев Д.К.,Бекназаров С.,Бағдаулет Д. Metasploit framework арқылы желі мен сервердегі осалдықтарды сканерлеу және операциялық жүйелерге қашықтан қол жеткізу.- Вестник КазУТБ.-2024- № 1(22).- С.97-106

Авторлар туралы мәліметтер

Бидахмет Ж. - PhD, әл-Фараби атындағы Қазақ ұлттық университетінің м.а. доценті, Алматы, Қазақстан,e-mail:bidakhmetzhanar@gmail.com;

Уайда А. – әл-Фараби атындағы Қазақ ұлттық университетінің магистранты, Алматы, Қазақстан, e-mail: uaida_a@mail.ru;

Бағдаулет Д. - әл-Фараби атындағы Қазақ ұлттық университетінің магистранты, Алматы, Қазақстан, e-mail: dasik-007@mail.ru;

Әлішер Р. - әл-Фараби атындағы Қазақ ұлттық университетінің магистранты, Алматы, Қазақстан, e-mail: roma43529@gmail.com;

Қаржаубаев Қ. - әл-Фараби атындағы Қазақ ұлттық университетінің магистранты, Алматы, Қазақстан, e-mail: Karzhaubayevkuanysh@gmail.com;

Сердалы А.- әл-Фараби атындағы Қазақ ұлттық университетінің магистранты, Алматы, Қазақстан, e-mail: altynayserdaly@gmail.com;

Ахметов Ә. - әл-Фараби атындағы Қазақ ұлттық университетінің магистранты, e-mail: Aahmetov755@gmail.com;

Information about authors

Bidakhmet Zh.- PhD,Acting Associate Professor NAO Al-Farabi Kazakh National University, Almaty, Kazakhstan, e-mail: bidakhmetzhanar@gmail.com;

Uaida A. - graduate student at Al-Farabi Kazakh National University, Almaty, Kazakhstan, e-mail: uaida_a@mail.ru;

Bagdaulet D. - graduate student at Al-Farabi Kazakh National University, Almaty, Kazakhstan,

e-mail: dasik-007@mail.ru;

Alisher R. -graduate student of Al-Farabi Kazakh National University, Almaty, Kazakhstan,

e-mail: roma43529@gmail.com;

Karzhaubaev K.- graduate student of Al-Farabi Kazakh National University, Almaty, Kazakhstan,

e-mail: Karzhaubayevkuanysh@gmail.com;

Serdaly A.-graduate student of Al-Farabi Kazakh National University, Almaty, Kazakhstan,

e-mail: altynayserdaly@gmail.com;

Akhmetov A.-graduate student of Al-Farabi Kazakh National University, Almaty, Kazakhstan,

e-mail:Aahmetov755@gmail.com