ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2025»

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2025»

2025
Астана

УДК 001(06)
ББК 72я631
F96

«ǴYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың XX Халықаралық ғылыми конференциясы = XX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2025» = The XX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2025». – Астана: – 3813 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-08-5373-7

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.В сборник вошли доклады студентов, магистрантов, докторантов имолодыхученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2025

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.2

Интеллектуальные информационные системы

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған аі дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «IOT Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

оперативно выявлять уязвимости и предотвращать угрозы, включая методы сокрытия информации с использованием стеганографии. В мае 2024 года было утверждено постановление правительства, определяющее новые требования по обеспечению информационной безопасности. Среди них – использование систем для предотвращения утечек данных (DLP), а также внедрение фильтрации сетевого трафика с применением межсетевых экранов. Эти инструменты повышают уровень защиты от скрытых методов передачи информации.

Таким образом, Казахстан активно совершенствует кибербезопасность, принимая законодательные инициативы, внедряя современные технологии и взаимодействуя с международными организациями.

Стеганография — это мощный инструмент, который может использоваться как для защиты данных, так и в целях кибератак. Для Казахстана важно не только применять стеганографию в области информационной безопасности, но и разрабатывать методы её выявления и предотвращения вредоносного использования. Развитие технологий обнаружения, законодательное регулирование и повышение осведомленности специалистов помогут Казахстану эффективно противостоять киберугрозам, связанным со стеганографией. Внедрение новых технологий и активное сотрудничество государственных и частных компаний в сфере кибербезопасности позволит укрепить цифровую защиту страны и минимизировать риски, связанные с использованием стеганографии в преступных целях.

Список использованных источников:

1. Кибербезопасность. Учебник для вузов. – Санкт-Петербург: Издательство ЛАНЬ, 2024. – 680 с.
2. Стеганографические методы защиты информации. – Москва: Издательство Картаслов, 2018. – 250 с.
3. Основы информационной безопасности и стеганографии: учебник и практическое руководство. – Казань: Издательство Казанского федерального университета, 2022. – 295 с.
4. Digital Watermarking and Steganography: Fundamentals and Techniques. – Boca Raton: CRC Press, 2017. – 292 p.

WI-FI ЖЕЛІСІНДЕ ШАҚЫРЫЛМАҒАН ҚОНАҚТАРДЫ АВТОМАТТЫ ТҮРДЕ АНЫҚТАУ ЖҮЙЕСІ

Танатаров Ернар, Іргебай Санжар, Султанов Алпамыс
ttt.ernar@gmail.com, irgebaikliptonit@gmail.com, salikovalpamys@gmail.com
Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті, Ақпараттық қаупсіздік кафедра студенттері Танатаров Ернар, Іргебай Санжар, Султанов Алпамыс топ 39,39/1
Астана, Қазақстан
Ғылыми жетекшісі – Казиева Н.М.

Аңдатпа: Бұл мақалада Wi-Fi желісіндегі рұқсатсыз қосылған құрылғыларды автоматты түрде анықтау жүйесі қарастырылады. Жүйе желідегі құрылғыларды бақылап, белгісіз MAC-адрестерді сенімді құрылғылар тізімімен салыстырады. Егер рұқсат етілмеген құрылғы анықталса, әкімшіге Telegram API арқылы жедел хабарлама жіберіледі. Python және Scapy құралдарының көмегімен жүзеге асырылған бұл жүйе ARP және DHCP сұраныстарын пайдаланып, желідегі құрылғылардың белсенділігін талдайды. Сонымен қатар, Kali Linux негізінде қауіпсіздік тесттері жүргізіліп, желінің қорғаныс деңгейі бағаланады. Ұсынылған шешім ұйымдар мен жеке тұлғалар үшін Wi-Fi инфрақұрылымының қауіпсіздігін нығайтуға

бағытталған. Жүйенің функционалын кеңейту мақсатында болашақта жасанды интеллектті қолдану арқылы құрылғылардың мінез-құлқын талдау мүмкіндігі қарастырылады.

Түйін сөздер: Wi-Fi қауіпсіздігі, желі әкімшілігі, рұқсатсыз қосылу, шақырылмаған қонақтарды анықтау, ақпараттық қауіпсіздік, ARP сұранысы, DHCP сұранысы, MAC-адрес, Telegram API, Python, Scapy, желіні сканерлеу, ақ тізім, құрылғыны бұғаттау, Kali Linux, желілік қауіптер, кибершабуыл, Nmap, желілік мониторинг, қауіпсіздік тестілеуі.

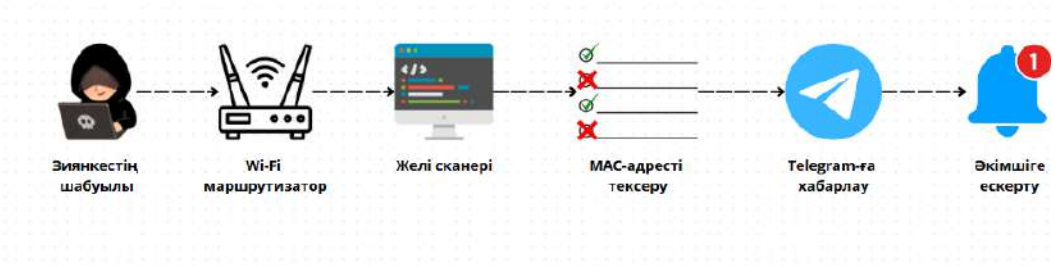
Қазіргі заманғы цифрлық ортада ақпараттық қауіпсіздікті қамтамасыз ету маңызды мәселелердің бірі болып табылады. Қауіпсіздік — бұл қашықтағы қызметтерге қол жеткізуге құқығы жоқ пайдаланушылардың оған талпынысын болдырмау[1, с. 807]. Цифрлық технологиялардың қарқынды дамуы және интернетке қосылу мүмкіндіктерінің кеңеюі ақпараттық қауіпсіздікке жаңа қауіптер туындатады. Соның ішінде, Wi-Fi желілерінің кең таралуы олардың қорғалу деңгейіне қойылатын талаптарды күшейтеді.

Wi-Fi желілері деректерді сымсыз тарату мүмкіндігі арқылы ыңғайлылық пен мобильділікті қамтамасыз етеді. Алайда, ашық және қорғалу деңгейі төмен Wi-Fi желілері кибершабуылдардың негізгі нысанасына айналады. Алаяқтар мұндай желілер арқылы пайдаланушылардың жеке деректеріне, банк карталарының мәліметтеріне және басқа да құпия ақпараттарына қол жеткізуі мүмкін. Wi-Fi желісіне белгісіз пайдаланушы кіріп кеткен жағдайда тіптен қиын болып кетеді, себебі ол сол әрекеті арқылы өзге пайдаланушылардың құйтырқы әрекеттеріне жол ашады. Интернет пайдаланушыларының адал екеніне сену – аңғалдық[2, с. 32] . Осыған байланысты шақырылмаған қонақтарды автоматты түрде анықтау жүйесін әзірлеу өзекті міндетке айналуда.

Бұл жүйе желідегі белсенді құрылғыларды бақылауға, рұқсатсыз қосылымдарды анықтауға және әкімшіге жедел хабарлама жіберуге мүмкіндік береді. Сонымен қатар, белгісіз құрылғыларды бұғаттау механизмі енгізіліп, желі қауіпсіздігін автоматтандыру шаралары қарастырылады. Жұмыс мысалыға MITM (Men in the middle) сияқты шабуылдармен Wi-Fi желісіне қосылмау үшін пайдалы қорғаныс түрі болуы мүмкін[3, с. 14]. Мұндай шешімдер ұйымдар мен жеке тұлғалар үшін Wi-Fi инфрақұрылымының қауіпсіздігін нығайтуға бағытталған. Жүйе Python және Scapy құралдарының көмегімен жүзеге асырылып, Telegram API арқылы хабарландырулар жіберу, iptables негізінде құрылғыларды бұғаттау және Kali Linux арқылы қауіпсіздік тесттерін жүргізу мүмкіндігін қамтиды. Бұл технологиялар кешені желіні қорғаудың тиімділігін арттырады және кибершабуылдарға қарсы тұрақтылығын қамтамасыз етеді.Желілік қауіпсіздік – бұл желі инфрақұрылымын және берілетін деректерді рұқсатсыз қол жеткізуден, шабуылдардан және істен шығудан қорғау практикасы [4, с. 657]. Ұсынылып отырған жүйе желіге рұқсатсыз қосылған құрылғыларды анықтап, олар туралы әкімшіні хабардар етуге арналған. Бұл келесі негізгі міндеттерді қамтиды:

1. **Желіде құрылғыларды анықтау** – ARP және DHCP сұраулары арқылы белсенді құрылғылардың MAC-адрестерін жинау.
2. **Ақ тізіммен салыстыру** – белгісіз MAC-адрестерді алдын ала анықталған сенімді құрылғылар тізімімен салыстыру.
3. **Хабарландыру жіберу** – Telegram бот арқылы әкімшіге күдікті құрылғылар туралы ескерту жіберу.

Сурет 1-де көрсетілген алгоритм жалпы Wi-Fi желісіне кіріп кеткен белгісіз пайдаланушыларды шығарып тастау процесін көрсетеді:



Сурет 1. Шақырылмаған қолданушыларды анықтау алгоритмі

```python
import telebot
import os
import logging
from detect import scan_network, load_whitelist, get_vendor, get_device_info

# Настройки Telegram-бота
TOKEN = "7751411172:AAGOZyx1i8oekNQOLM9REOEm1iVZ98"
CHAT_ID = "-100275818"
bot = telebot.TeleBot(TOKEN)

# Настройка логирования
logging.basicConfig(filename="network_alerts.log", level=logging.INFO, format="%(asctime)s - %(message)s")

# Файл заблокированных устройств
BLOCKED_FILE = "blocked_devices.txt"

def log_event(event):
    """Записывает события в лог."""
    logging.info(event)

def is_already_blocked(mac):
    """Проверяет, был ли MAC-адрес уже заблокирован."""
    if os.path.exists(BLOCKED_FILE):
        with open(BLOCKED_FILE, "r") as f:
            blocked_macs = f.read().splitlines()
        return mac in blocked_macs
    return False

def save_blocked_mac(mac):
    """Сохраняет MAC-адрес в файл заблокированных устройств."""
    with open(BLOCKED_FILE, "a") as f:
        f.write(mac + "\n")

def block_device(mac):
    """Блокировка устройства по MAC-адресу через iptables и nftables."""
    if is_already_blocked(mac):
        bot.send_message(CHAT_ID, f"⚠ Устройство с MAC {mac} уже заблокировано.")
        return

    # Блокировка через iptables
    os.system(f"iptables -A INPUT -m mac --mac-source {mac} -j DROP")
    os.system(f"iptables -A FORWARD -m mac --mac-source {mac} -j DROP")
    os.system(f"iptables -A OUTPUT -m mac --mac-source {mac} -j DROP")

    # Блокировка через nftables (если доступно)
    os.system(f"nft add rule ip filter input ether saddr {mac} drop")

    # Сохранение в файл
    save_blocked_mac(mac)

    # Логирование и сообщение
    bot.send_message(CHAT_ID, f"⛔ Устройство с MAC {mac} заблокировано!")
    log_event(f"Blocked device: {mac}")

def alert_admin(device):
    """Отправляет уведомление о неизвестном устройстве и логирует событие."""
    vendor = get_vendor(device['mac'])
```

Сурет 2. telegram_alert.py скрипты

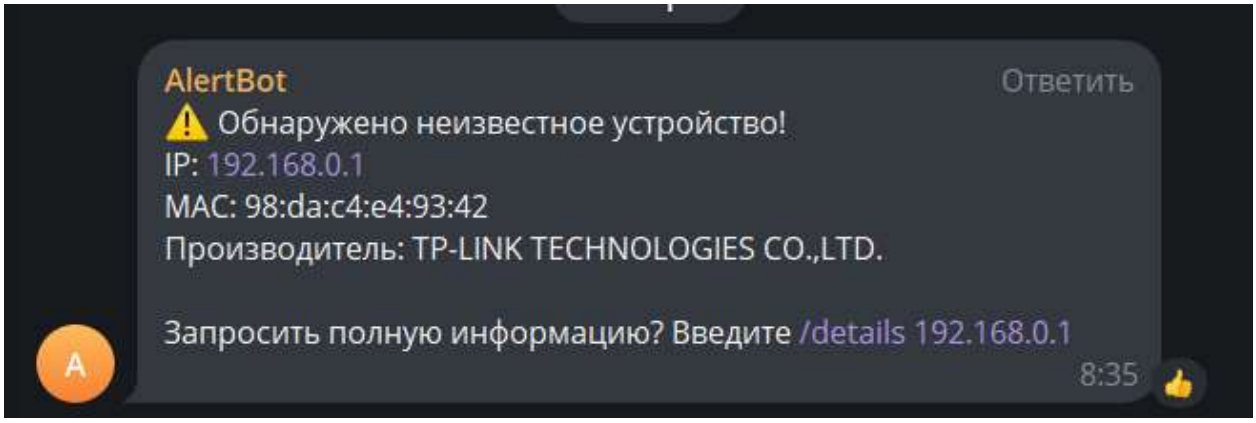
Бұл скрипт Wi-Fi желісіндегі белгісіз құрылғыларды автоматты түрде анықтап, Telegram арқылы әкімшіге хабарлама жібереді. Бағдарлама алдымен рұқсат етілген құрылғылардың тізімін (whitelist) жүктейді, содан кейін scan_network() функциясы арқылы желіні сканерлейді. Егер құрылғы whitelist тізімінде болмаса, оның MAC және IP мекенжайлары, өндірушісі туралы ақпаратпен бірге Telegram-ға хабарлама жіберіледі. Әкімші /details <IP> командасы арқылы қосымша ақпарат ала алады немесе /block <MAC> командасын қолданып, құрылғыны iptables және nftables арқылы бұғаттай алады. Сондай-ақ, /whitelist <MAC> командасы арқылы құрылғыны рұқсат етілгендер тізіміне қосуға болады, ал /network командасы желідегі барлық құрылғылардың тізімін көрсетеді. Бот блокталған құрылғылардың

тізімін blocked_devices.txt файлына сақтайды және барлық әрекеттерді network_alerts.log журналына жазады. Егер желіде бөтен құрылғылар табылмаса, бот Telegram-ға "В сети нет неизвестных устройств. Всё чисто." хабарламасын жібереді. Бағдарлама тұрақты жұмыс істеп, желіні үнемі бақылап отырады.

Список разрешенных MAC-адресов
1a:2b:3c:4d:5e:6f
7d:8e:9f:0a:1b:2c
9a:0b:1c:2d:3e:4f
5a:6b:7c:8d:9e:0f

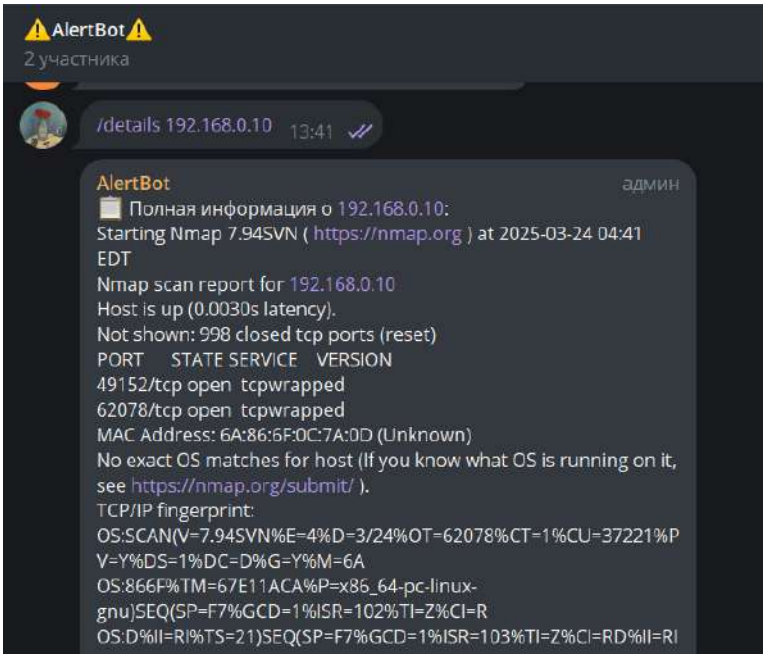
Рұқсат етілген MAC адрестер тізімі

Бұл бізде рұқсат етілген MAC адрестердің тізімі, яғни егер осы MAC адрестерден бөлек MAC адрес табылса телеграм арқылы уведомление келеді.



Сурет 3. Телеграмға келетін хабарлама түрі

AlertBot анықталмаған құрылғыны тапты және әкімшіге Telegram арқылы хабарлама жіберді. Хабарламада құрылғының IP-адресі (192.168.0.1), MAC-адресі (98:da:c4:e4:93:42) және өндірушісі (TP-LINK TECHNOLOGIES CO., LTD.) көрсетілген. Сонымен қатар, толық ақпарат алу үшін /details 192.168.0.1 командасын енгізу ұсынылады. Бұл жүйе желідегі бейтаныс құрылғыларды бақылауға және әкімшіге жылдам хабарлауға мүмкіндік береді.



Сурет 4. details командасы арқылы белгісіз құрылғы жайлы толық ақпарат алу

AlertBot толық ақпаратты ұсынды, ол 192.168.0.10 құрылғысына Nmap утилитасы арқылы сканерлеу жүргізді. Есепте құрылғының желіде белсенді екені (Host is up) және оның екі ашық порты бар екені (49152/tcp және 62078/tcp) көрсетілген. MAC-адресі 6A:86:6F:0C:7A:0D, бірақ өндірушісі анықталмаған. Операциялық жүйені нақты сәйкестендіру мүмкін болмады, бірақ TCP/IP fingerprinting нәтижелері көрсетілген. Traceroute нәтижесіне сәйкес, құрылғы желіде бір аралықтан кейін қолжетімді. Бұл ақпарат желі әкімшісіне құрылғының ашық порттарын және белсенділігін бақылауға көмектеседі.

Қорытынды. Бұл зерттеу жұмысы Wi-Fi желісінде шақырылмаған қонақтарды автоматты түрде анықтау жүйесін әзірлеуге арналған. Қазіргі таңда ақпараттық қауіпсіздік маңызды мәселе болып табылады, және ұсынылған шешім желіге рұқсатсыз қосылған құрылғыларды анықтап, әкімшіге хабарлау арқылы қауіпсіздікті арттыруға бағытталған. Жүйе Python және Scapy кітапханаларының көмегімен жүзеге асырылып, ARP және DHCP сұраулары арқылы белсенді құрылғыларды анықтайды. Белгісіз құрылғылар сенімді құрылғылар тізімімен салыстырылып, сәйкессіздік анықталған жағдайда Telegram API арқылы әкімшіге хабарлама жіберіледі. Сонымен қатар, Kali Linux жүйесі негізінде жүргізілетін қауіпсіздік тесттері желінің қорғаныс деңгейін бағалауға мүмкіндік береді. Detect.py және Telegram_alert.py скрипттерінің үйлесімді жұмысы құрылғыларды анықтау, өндірушілерін талдау және қосымша желілік ақпарат алу процесін автоматтандырады. Егер белгісіз құрылғы анықталса, әкімші оның IP және MAC мекенжайлары, өндірушісі, ашық порттары және желідегі белсенділігі туралы толық мәлімет ала алады. Бұл жүйе ұйымдар мен жеке тұлғалар үшін киберқауіптерге қарсы қосымша қорғаныс қабатын қамтамасыз етеді. Сонымен қатар біздің әзірлеген қорғау жүйеміз шағын яғни көп шығынды, қымбат құрылғыларды қолдануға мүмкіндік болмаған wi-fi желілерінде де жұмыс жасайды. Осылайша, әзірленген жүйе Wi-Fi желілерін рұқсатсыз пайдаланудан қорғауға мүмкіндік береді және ақпараттық қауіпсіздікті нығайтуға бағытталған тиімді құрал болып табылады. Болашақта оның функционалын кеңейтіп, жасанды интеллект негізінде құрылғылардың мінез-құлқын талдау мүмкіндігін қосуға болады.

Пайдаланылған әдебиеттер тізімі

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. – 5-е изд. – СПб.: Питер, 2012. – 960 с. [https://kr-labs.com.ua/books/Tenenbaum_KS.pdf]
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. – 2-е изд. – М.: Триумф, 2006. – 816 с. [https://kr-labs.com.ua/books/Bryus_Shnayer_-_Prikladnaya_Kriptografia.pdf]
3. Лапонина О.Р. Основы сетевой безопасности. – Национальный Открытый Университет «ИНТУИТ» , 2014. – 384 с [http://master.cmc.msu.ru/files/Laponina-1.pdf]
4. Kurose J., Ross K. Computer Networking: A Top-Down Approach. – 7th ed. – Pearson, 2017. –912p. [https://www.ucg.ac.me/skladiste/blog_44233/objava_64433/fajlovi/Computer%20Networking%20_%20A%20Top%20Down%20Approach,%207th,%20converted.pdf]
5. Kali Linux операциялық жүйесі [https://www.kali.org/get-kali/#kali-platforms]
6. NMAP утилитасы [https://nmap.org/download]
7. Telegram әлеуметтік желісі [https://web.telegram.org/]

ФИШИНГ: ЖЕЛІДЕГІ BEEF ӘДІСІ АРҚЫЛЫ АЛДАУ ЖӘНЕ ОДАН САҚТАНУ

Таубай М.Е. Раматуллаев Ә.А.
Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
Астана, Қазақстан.
maditaubay04@gmail.com alimramatullaev@gmail.com

Аңдатпа

Бұл мақалада біз сілтеме арқылы шабуыл жасау түрлерін қарастырамыз. Біздің қарастыратындарымыз фишинг және BeEF (Browser Exploitation Framework), сондай-ақ екеуінің өзара байланысын және осы қауіптерден қорғану әдістерін талдаймыз. Хакерлердің BeEF-ті қалай өздеріне тиімді етіп пайдаланатынын және пайдаланушылар мен ұйымдардың осы шабуылдарға төтеп бере алатындай қандай қадамдар жасайтынын талқылаймыз.

Кілттік сөздер: фишинг, әлеуметтік инженерия, BeEF, интернет қауіпсіздігі, киберқауіп, қорғаныс әдістері.

1. Кіріспе

Интернеттегі қауіптер күн сайын күрделене түсуде, ал киберқылмыскерлер пайдаланушылардың жеке деректерін алу үшін жаңа әдістерді қолдануда. Солардың ішінде ең көп тарағаны – **фишинг**. Бұл – алаяқтықтың кең таралған түрі, оның көмегімен қаскүнемдер логиндер, парольдер, банк карталарының деректері сияқты маңызды ақпаратты қолға түсіреді. Сонымен қатар, **BeEF (Browser Exploitation Framework)** құралы веб-шолғыштардың осалдықтарын пайдаланып, шабуылдаушыларға қосымша артықшылықтар береді.[1]

Фишингтің қаупі

Фишингтің басты қаупі – оның адамдарды алдау арқылы жүзеге асуы, сондықтан одан толық қорғану қиын. Компаниялар ақпараттық қауіпсіздік бойынша оқыту жүргізсе де, алаяқтар өз әдістерін жетілдіріп отырады.

Фишингтің тағы бір қатері – құпия деректердің қолды болуы. Егер **логин мен құпиясөз** ұрланса, қолданушы аккаунтынан айырылуы мүмкін. **Банк картасының мәліметтері** түссе, алаяқтар қаржыны иемденуге тырысады. Ал жеке ақпарат көбіне **үшінші тараптарға сатылады, интернетте жарияланады** немесе **қосымша шабуылдарға қолданылады**.[2]