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

күйінде берілуі жүйенің осалдығын арттырады. Бұл MITM (Man-in-the-Middle) шабуылдары мен деректердің ұрлану қаупін тудырады.

Желілік қауіпсіздікті арттыру үшін шифрлау механизмдерін күшейту, аутентификацияны жетілдіру және желілік трафикті үнемі бақылау қажет. TLS 1.3 және Perfect Forward Secrecy технологияларын қолдану деректердің қауіпсіздігін қамтамасыз етеді. Сонымен қатар, HTTP Strict Transport Security механизмі арқылы MITM шабуылдарының алдын алуға болады. Құпиясөздерді серверге жібермес бұрын хештеу және қосымша аутентификация әдістерін енгізу пайдаланушы деректерін қорғаудың тиімді әдістері болып табылады.

Жалпы, Wireshark сияқты құралдарды тиімді пайдалану ұйымдардың ақпараттық қауіпсіздігін нығайтуға және ықтимал киберқауіптерден қорғануға мүмкіндік береді. Дұрыс конфигурацияланған желілік қауіпсіздік жүйесі шабуылдардың алдын алуға және маңызды деректерді қорғауға көмектеседі.

Қолданылған әдебиеттер тізімі

1. Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.
2. Bejtlich, R. (2004). *The Tao of Network Security Monitoring: Beyond Intrusion Detection*. Addison-Wesley.
3. Sanders, C. (2017). *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems* (3rd ed.). No Starch Press.
4. Orebaugh, A., Ramirez, G., Beale, J., Burke, J., & Wright, L. (2006). *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Syngress.
5. Scarfone, K., & Mell, P. (2009). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. National Institute of Standards and Technology (NIST).
6. Chappell, L. (2017). *Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide* (2nd ed.). Protocol Analysis Institute.
7. Stallings, W. (2020). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson.

MITM ШАБУЫЛЫ ТУРАЛЫ

Кәкімбек Әділ Қайроллаұлы, Серікбай Ақжол Ерболатұлы, Наурызбаев Дарын Ерболатұлы

Л.Н.Гумилев атындағы ЕҰУАқпараттық технологиялар факультетінің ақпараттық қауіпсіздік жүйелерінің оқытушысы, Астана, Қазақстан

Ғылыми жетекшісі – Н.Казиева

Ортадағы адам (MITM) шабуылы – шабуылдаушы тікелей байланысып жатыр деп есептейтін екі тарап арасындағы байланысты ұстап алатын және ықтимал өзгертетін кибершабуыл түрі.[3] MITM шабуылдарының табиғатын, оларды анықтау және алдын алу әдістерін және нақты әлемде қолдану жағдайларын тереңірек түсіну үшін келесі мақалаларды оқуды ұсынамыз: «Ортадағы адам: анықтау және алдын алу бойынша кеңестер» Habr TM шабуылдарының егжей-тегжейлері мен қорғау механизмдері туралы мақалаларды оқып шығуды ұсынамыз . [2] «Ортадағы адам туралы (MitM) шабуылы» «Ортадағы адам» шабуылының теориялық және практикалық аспектілеріне, сондай-ақ олардың алдын алу әдістеріне арналған аналитикалық материал. [2] “Ортадағы адам (MITM) шабуылы дегеніміз

не? Анықтамасы және алдын алу” MITM шабуылдарының сипатын түсіндіретін және олардың алдын алу шараларын ұсынатын мақала. [1] "Орта шабуылдардағы адам (MIMA) дегеніміз не?"

MITM шабуылдарының сипатын және олармен байланысты тәуекелдерді сипаттайтын ICANN ұсынған материал. [3]

Man-in-the-Middle (MITM) шабуылдары ақпараттық қауіпсіздікке үлкен қауіп төндіреді. Төменде мұндай шабуылдардың іс жүзінде қалай жүзеге асырылғанын көрсететін кейбір нақты жағдайлар берілген:

1. Comcast Ad Embedding: 2014 жылы Comcast пайдаланушылар кірген веб-беттерге өзінің JavaScript кодтарын енгізу үшін MITM әдістерін пайдаланғаны анықталды. Бұл компанияға өзінің жарнамалары мен хабарламаларын үшінші тарап веб-беттерінің үстінде көрсетуге мүмкіндік беріп, пайдаланушының құпиялылығы мен қауіпсіздігіне қатысты алаңдаушылық туғызды. [3]

2. Lenovo ноутбуктеріндегі Superfish оқиғасы: 2014 жылы Lenovo өз ноутбуктерінде Superfish Visual Search бағдарламалық құралын алдын ала орнатқан. Бағдарламалық жасақтама шифрланған HTTPS трафигін ұстау үшін MITM шабуылын қолданды, бұл пайдаланушылардың іздеу нәтижелеріне өз жарнамаларын енгізуге мүмкіндік берді. Мұндай араласу пайдаланушылардың жеке деректерінің бұзылу қаупіне ұшырады. [4]

3. Ұлыбритания теміржол вокзалындағы Wi-Fi шабуылы: 2024 жылдың тамыз айында Ұлыбританияның ірі теміржол вокзалдарында жолаушылар тегін Wi-Fi желісіне қосылу кезінде террористік қауіптерге қатысты хабарларға тап болды. Тергеу нәтижесінде Wi-Fi провайдерінің қызметкері рұқсат етілмеген өзгертулер енгізіп, нәтижесінде мұндай хабарламалар пайда болғаны анықталды. [5]

4. Испаниядағы қаржылық алаяқтық: 2025 жылдың ақпанында Испанияның Алькала-де-Хенарес қаласында MITM алаяқтық жасағаны үшін ер адам қамауға алынды. Ол қызмет көрсетушінің электрондық пошта мекенжайын қолдан жасап, төлеуші компанияны басқа банк шотына шамамен 175 000 еуро аударуға көндірді, бұл айтарлықтай қаржылық шығын келтірді. [6]

Жоғарыда қарастырылған MITM шабуылын мысал ретінде қарастырдық.

Зерттеу барысында біз MITM шабуылын жасау үшін Radmin VPN қосымшасы арқылы виртуалды локальды желі құрдық.

1 - суретте сервер қосымшасының интерфейсі көрсетілген. Сервер клиенттен қосылуды күтеді. Клиент қосылғаннан кейін олардың арасында хабарламалар алмасылады. Әрбір клиент жіберген хабарлама экранға шығады және сервер оған жауап қайтарады.

1-сурет. B (сервер) көрінісі

Код құрылысы:

Сервер сокетін құру (порт 9000):

Клиенттің қосылуын күту

Клиент қосылды (IP, портты көрсету)

Әңгімелесу циклі:

Клиенттен хабарлама алу

Егер хабарлама жоқ болса, байланысты жабу

Хабарламаны экранға шығару

Сервер (сен) хабарлама жазу

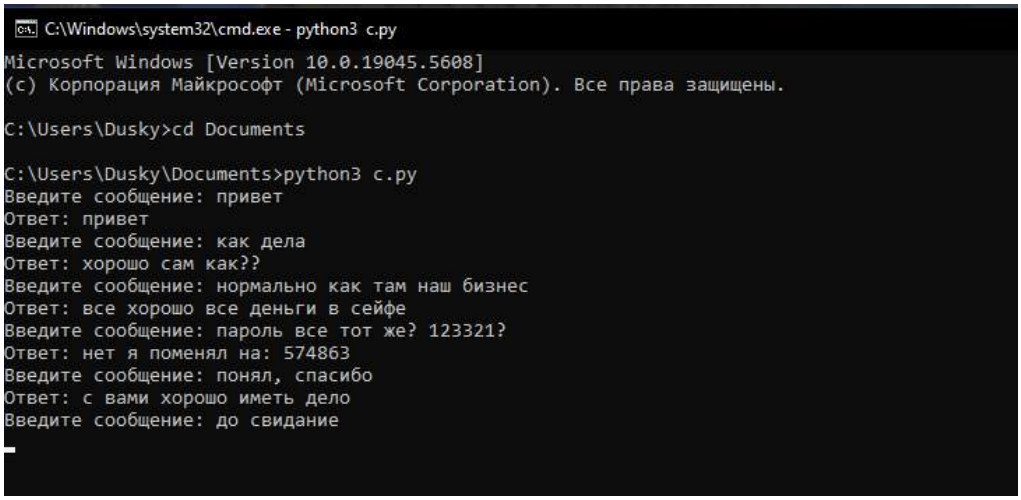
Егер хабарлама "exit" болса, байланысты жабу

Хабарламаны клиентке жіберу

Егер байланыс үзілісі болса, қатені шығарып, байланысты жабу

Сервердің жұмысын тоқтату

2 - суретте клиенттің қосымша интерфейсі көрсетілген. Клиент сервермен байланыс орнатады, содан кейін хабарламалар енгізіп серверге жіберіп отырады. Сервердің жауабын қабылдап, экранға шығарады.



2-сурет. А (клиент) көрінісі

Код құрылысы:

Сервермен байланыс орнату (IP: 26.49.11.123, порт: 9000):

Әңгімелесу циклі:

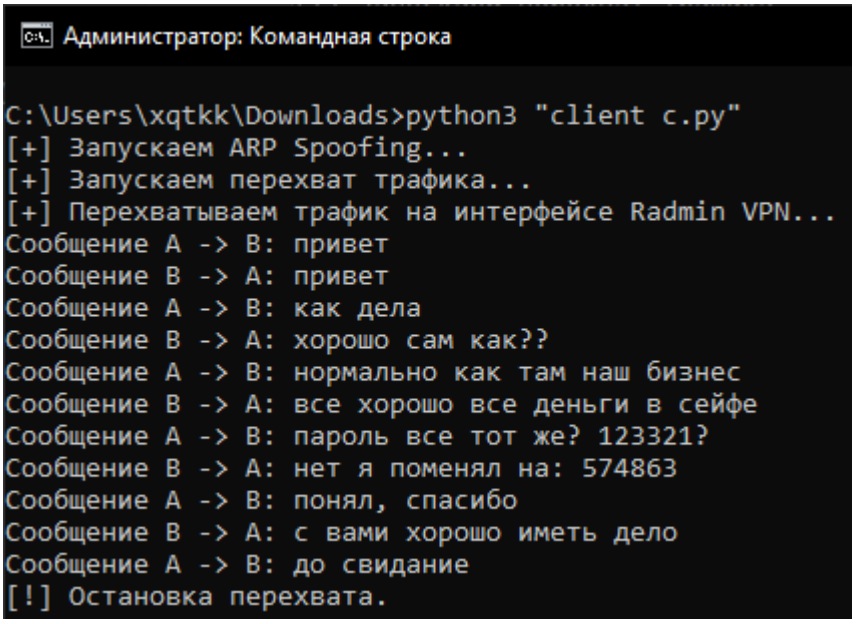
Хабарламаны енгізу

Хабарламаны серверге жіберу

Серверден жауап алу

Жауапты экранға шығару

3 - суретте хакердің MITM шабуылын іске асыратын интерфейсі көрсетілген. Ол ARP spoofing арқылы клиент пен сервер арасындағы хабарламаларды тыңдап, олардың арасында жүретін ақпаратты көре алады.



3-сурет. С (хакер) көрінісі

Код құрылысы:

Бастапқы параметрлер:

Клиенттің (A) және сервердің (B) IP-адрестерін көрсету

VPN интерфейсін таңдау (Radmin VPN)

ARP Spoofing процесін іске қосу:

Әр 2 секунд сайын қайтала:

Клиентке жалған ARP жауап (\"мен сервермін\")

Серверге жалған ARP жауап (\"мен клиентпін\")

Трафикті ұстау және өңдеу:

Желіден пакетті ұстап алу

Егер пакет TCP 9000 портына бағытталған болса:

Пакеттің бағытын анықтау (A→B немесе B→A)

Пакет мазмұнын экранға шығару (хабарлама)

Пакетті қайта жинап, қарсы тарапқа жіберу (байланысты сақтау)

Процесті тоқтату (пернетақтадан сигнал берілгенде)

Қалай іске асырылды:

Жүйеде үш негізгі түйін жұмыс істейді:

- Сервер (B) клиенттің қосылуын күтіп, байланыс орнатады.
- Клиент (A) серверге қосылып, хабарлама алмасады.
- Хакер (C) ARP spoofing техникасын пайдаланып, клиент пен сервер арасында деректерді ұстап, бақылауға алады.

Бұл арқылы хакер (C) клиент (A) мен сервер (B) арасындағы барлық сөйлесуді көре алады және қажетті ақпаратты оңай ала алады.

Төмендегі шаралар арқылы MITM (Man-in-the-Middle) шабуылдарының тәуекелін айтарлықтай төмендетуге болады:

1. Шифрлауды қолдану:

- HTTPS протоколын пайдаланыңыз, SSL/TLS сертификаттарын қолданыңыз.
- Күшті шифрлау алгоритмдерін қолданыңыз.

2. ARP spoofing-тен қорғану:

- Желілік деңгейде ARP spoofing-ке қарсы ARP inspection, DHCP snooping, IP Source Guard сияқты механизмдерді қолданыңыз.

- Статикалық ARP-кестесін қолданыңыз (тек сенімді желілерде мүмкін).

3. VPN-ды қолдану:

- VPN арқылы барлық деректерді шифрлап, сенімді арналар арқылы жіберіңіз.
- Сенімді VPN қызметтерін қолданыңыз.

4. Қауіпсіз желілерді пайдалану:

- Ашық Wi-Fi желілерін пайдаланбаңыз немесе қолданған жағдайда VPN қосылыңыз.
- Қауіпсіздік шаралары бар және сенімді желілерді қолданыңыз.

5. Бағдарламалық қамтамасыз етуді жаңарту:

- Қолданылатын бағдарламалық жасақтамаларды (операциялық жүйелер, браузерлер және т.б.) үнемі жаңартып отырыңыз.
- Жаңартуларда анықталған осалдықтар жөнделеді.

6. Қауіпсіздік саясаттарын енгізу:

- Желіде қауіпсіздік саясатын қолданыңыз.
- Қызметкерлерді MITM шабуылдары туралы ескертіп, ақпараттық қауіпсіздікке үйретіңіз.

Қорытынды

MITM шабуылы – шабуылдаушы тараптың клиент пен сервер арасындағы деректер алмасуын ұстап алу, өзгерту немесе бағыттау арқылы жүзеге асырылатын қауіпті кибершабуылдардың бірі. Бұл зерттеуде біз MITM шабуылының негізгі түрлерін, олардың нақты өмірдегі мысалдарын және шабуылдарды іске асыру әдістерін қарастырдық.

Симуляцияда Radmin VPN көмегімен виртуалды желі құрып, ARP spoofing әдісі арқылы MITM шабуылын модельдедік. Эксперимент нәтижелері көрсеткендей, егер тиісті қорғаныс шаралары қолданылмаса, шабуылдаушы желідегі ақпаратты оқып, өзгерте алады.

MITM шабуылдарынан қорғану үшін келесі қауіпсіздік шараларын қолдану қажет: шифрлау (SSL/TLS), ARP spoofing-тен қорғану әдістері, VPN қолдану, қауіпсіз желілерге қосылу, бағдарламалық жасақтаманы үнемі жаңарту және қауіпсіздік саясаттарын енгізу.

Зерттеу нәтижелері MITM шабуылының күрделілігін және оған қарсы қорғанудың маңыздылығын тағы да дәлелдейді. Ақпараттық қауіпсіздікті қамтамасыз ету үшін тиісті шараларды уақытылы қабылдау қажет.

Қолданылған әдебиеттер тізімі;

1. Что такое атаки типа «злоумышленник в середине» или, как их еще называют, атаки посредника (Man in the Middle Attack, MIMA)? (https://www.icann.org/ru/blogs/details/what-is-a-man-in-the-middle-attack-2-11-2015-ru)
2. Все об атаке “Человек по середине” (Man in the middle, MitM) https://www.anti-malware.ru/analytics/Threats_Analysis/man-in-the-middle-attack
3. Man-in-the-middle attack (https://en.wikipedia.org/wiki/Man-in-the-middle_attack)
4. Man-in-the-Middle (MITM) Attack: Definition, Examples & More (https://www.strongdm.com/blog/man-in-the-middle-attack)
5. Train passengers see terror messages after station wi-fi hack (https://www.thetimes.co.uk/article/train-passengers-islamist-terror-messages-wifi-hack-ld78vqjr0)
6. Detenido en Alcalá de Henares por hacer el “man in the middle” (https://cadenaser.com/cmadrid/2025/02/11/detenido-en-alcala-de-henares-por-hacer-el-man-in-the-middle-ser-henares)