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

4. National Institute of Standards and Technology (NIST). Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. December 2016. 23 p. (URL: https://csrc.nist.gov/Projects/post-quantum-cryptography)

5. Cherkaoui Dekkaki, K.; Tasic, I.; Cano, M.-D. Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process. Technologies 2024, 12, 241. https://doi.org/10.3390/ technologies12120241

6. Barton M., et al. Benchmarking Post-Quantum Cryptography on ARM Cortex-M // Cryptographic Hardware and Embedded Systems - CHES 2021. 2021. P. 319-338.

7. Cherkaoui Dekkaki S., El Idrissi N., Ez-Zahraouy H. Comparative analysis of post-quantum cryptographic algorithms for IoT security // Journal of Information Security and Applications. 2024. Vol. 78. P. 103678. (DOI: 10.1016/j.jisa.2024.103678)

8. Bindel N., Schanck J.M., Schuldt J.C.N., Veitch D. Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange // Post-Quantum Cryptography. PQCrypto 2019. Lecture Notes in Computer Science, vol 11505. Springer, Cham. 2019. P. 206-226.

УДК 004.056.5

ЗАМАНАУИ ОПЕРАЦИЯЛЫҚ ЖҮЙЕЛЕРДЕГІ ЖАДЫ ДАМПЫ КЕСКІНІН АЛУ ҚҰРАЛДАРЫН ТАЛДАУ ЖӘНЕ САЛЫСТЫРУ

Жолдасбаев Мағжан Әбілтайұлы
magzhanzholdasbaev@mail.ru
Л.Н.Гумилев атындағы ЕҰУ «Ақпараттық технологиялар» факультетінің 2-курс магистранты, Астана, Қазақстан
Ғылыми жетекшісі – Ж.Сауханова

Қазіргі ақпараттық жүйелер жоғары архитектуралық күрделілікпен және өңделген деректердің айтарлықтай көлемімен сипатталады. Мұндай жағдайларда жедел жад күйін талдау келесі мәселер үшін өте маңызды болып табылады:

1) Критикалық ақауларды диагностикалау және ақаулықтарды жою (BSOD, kernel panic)

2) Ақпараттық қауіпсіздік инциденттерін зерттеу

3) Цифрлық деректерді криминалистикалық талдау

Дәстүрлі тіркеу әдістері жүйенің ақаулық кезіндегі жағдайын толық түсіну үшін жиі жеткіліксіз және бұл жады дампын қажет ақпарат көзі етеді.

Жады дампы әдетте жүйе қатесі немесе бағдарлама ақауы орын алған кезде автоматты түрде жасалады. Бұл дампты пайдалану арқылы жүйенің немесе бағдарламаның қай жерінде ақау болғанын анықтауға болады.

Жады дампын бірнеше негізгі критерийлер бойынша жіктеуге болады, оның ішінде егжей-тегжейлі зерттеу деңгейі , қол жеткізу мақсаты, кескінін алу әдісі және сақтау пішімі бойынша қарастырылады. Төменде егжей-тегжейлі жүйелеу көрсетілген.

1. Жады дампын мәліметтерді толық қамту деңгейі бойынша жүйелеу

1.1. Толық жад дампы жүйенің жадындағы барлық деректердің көшірмесі, ол жүйенің жұмыс істеп тұрған бағдарламалары мен компоненттерінің жағдайын сақтайды. Дампта процессорлардың регистрлері, бағдарламалардың және драйверлердің ішкі күйі туралы ақпараттар болады. Бұл дамп ақауларды терең зерттеуге мүмкіндік береді, себебі барлық жүйелік деректер қамтылады. Дегенмен, оның көлемі үлкен болуы мүмкін, бұл оны сақтау мен өңдеуді қиындатады. Толық жад дампы күрделі қателіктер мен құлдырауларды анықтауға

көмектеседі. Ол жүйенің ішкі жұмысын талдауға, сондай-ақ жүйені оңтайландыру және тұрақтылығын қамтамасыз ету үшін маңызды. Бұл құрал бағдарламалау, жүйелік диагностика, ақпараттық қауіпсіздік және серверлік жүйелерде де қолданылады.Толық жады дампын алуға арналған құралдар ретінде мыналарды қарастыруға болады:

a) Windows: WinDbg (.dump /ma), Belkasoft RAM Capturer;
b) Linux: dd + /dev/mem, LiME;
c) macOS: osxpmem;

1.2. Ядро дампы жүйенің ядросының жұмысын сипаттайтын жадтың көшірмесі, ол жүйе құлаған кезде автоматты түрде жасалады. Бұл дамп тек жүйелік деңгейдегі деректерді, атап айтқанда, ядроның күйі мен драйверлердің жұмысын қамтиды. Талдау арқылы жүйе әкімшілері немесе бағдарламашылар ядроның ақауын анықтап, оны түзету жолдарын іздей алады. Ядро дампы жүйенің тұрақтылығын қамтамасыз ету және жүйелік ақауларды жөндеу үшін қолданылады. Сонымен қатар, ол жүйенің қауіпсіздігін жақсарту мақсатында жүйелік ақауларды зерттеуге арналған құрал болып табылады. Дампта ядроның күйі, жүйелік деректер, драйверлер мен модульдер, сондай-ақ қате туралы ақпарат қамтылады. Кейде ядро дампы пайдаланушы кеңістігіндегі маңызды деректерді де сақтап, жүйенің құлдырауы немесе қатесі туралы қосымша ақпарат береді. Толық дамппен салыстырғанда артықшылығы өлшемі анағұрлым аз әрі драйверлермен критикалық қателелерді диагностикалауға жеткілікті.

Аталған дамптың кескіні алу құралдарына мысал ретінде:

a) Windows: Control Panel → System → Advanced → Startup and Recovery баптауын;
b) Linux: kdump + crash утилитасын қарастыруға болады.

1.3. Минидамп (Small Memory Dump)

Минималды жад дампы (минидамп) жүйенің жұмыс істеп тұрған кезінде тек ең маңызды ақпаратты қамтитын шағын жад көшірмесі болып табылады. Бұл дамп жүйенің негізгі күйін, процесс идентификаторын және қатенің орын алған жерін ғана көрсетеді, сондықтан ол толық жад дампына қарағанда әлдеқайда аз орын алады. Минималды жад дампы жүйелік немесе бағдарламалық қателерді жылдам анықтауға мүмкіндік береді, бірақ толық терең талдауды қамтамасыз етпейді. Минималды жад дампының негізгі артықшылығы жылдам талданады және ресурстарды үнемдейді. Бұл дамп жүйе деңгейіндегі ақауларды тез анықтау үшін пайдалы, себебі ол тек маңызды ақпаратты сақтайды. Сонымен қатар, минималды жад дампының қолданылуы қарапайым әрі жиі кездесетін жүйелік қателерді зерттеуге ыңғайлы.

Минидамп кескінін алушы құралдарға:

a) Windows: Minidump (WER жүйесінде конфигурацияланады)
b) Linux: systemd-coredump

1.4. Пайдаланушы процесінің дампы (User-mode Process Dump)

Пайдаланушы процесінің дампы жүйе қатесі немесе құлдырауы кезінде пайдаланушы кеңістігіндегі процестің жадын сақтайтын файл.. Дампта процестің стек деректері, жадының мазмұны, регистрлер мен айнымалылар сияқты маңызды ақпараттар сақталады. Бұл дампты пайдалану арқылы бағдарламашылар процестің қателіктерін анықтап, түзету жолдарын таба алады. Оның көлемі бірнеше мегабайттан аспайды, бұл оны өңдеуді жеңілдетеді. Дампта процесс идентификаторы (PID) мен қате туралы ақпарат, сондай-ақ сигналдар мен кідірістер туралы мәліметтер де болуы мүмкін.Дампты қолға түсіруге арналған құралдарға мыналар жатады:

a) Windows: ProcDump, Task Manager;
b) Linux: gcore, gdb;
c) macOS: lldb + process save-core;

2. Жады дампын алу мақсаты бойынша жүйелеу

Бұл кесте жадтың дампын алу мақсатында қолданылатын құралдар мен операциялық жүйелерді көрсетеді, ал әрбір мақсаты бойынша сәйкес критерийлер анықталған.

Құрал түрі	Мақсаты	Құралдар	Операциялық жүйе
Түзету	Бағдарламалық жасақтамадағы қателерді іздеу, жадтың ағып кетуін талдау	WinDbg, gdb, lldb	**Windows, Linux, macOS**
Криминалистикалық	Зиянды бағдарламалардың іздерін іздеу, артефактілерді алу	Volatility, LiME, Rekall	**Windows, Linux**
Өнімділік	Қолданбаның өнімділігін оңтайландыру, жадты пайдалануды талдау	ProcDump, perf (Linux), Instruments (macOS)	**Windows, Linux, macOS**
Жүйелік	BSOD/kernel panic диагностикасы, драйверді талдау	kdump, WinDbg, crash	**Linux, Windows**

Кесте 1. Жады дампының кескіні алу құралдарының мақсаты бойынша жіктелуі.

3. Құралдар көмегімен жады дампын қолға түсіру процессі

3.1. Ядро дампын алу LiME (Linux Memory Extractor) құралы

```
[root@mag ~]# insmod lime-2.6.32-431.5.1.el6.x86_64.ko "path=/root/mem.img format=lime"

[root@mag ~]# ls -lah /root/mem.img
-r--r--r--. 1 root root 1.0G Mar 9 08:11 /root/mem.img
```

Сурет 1. Ядро дампын алу барысы.

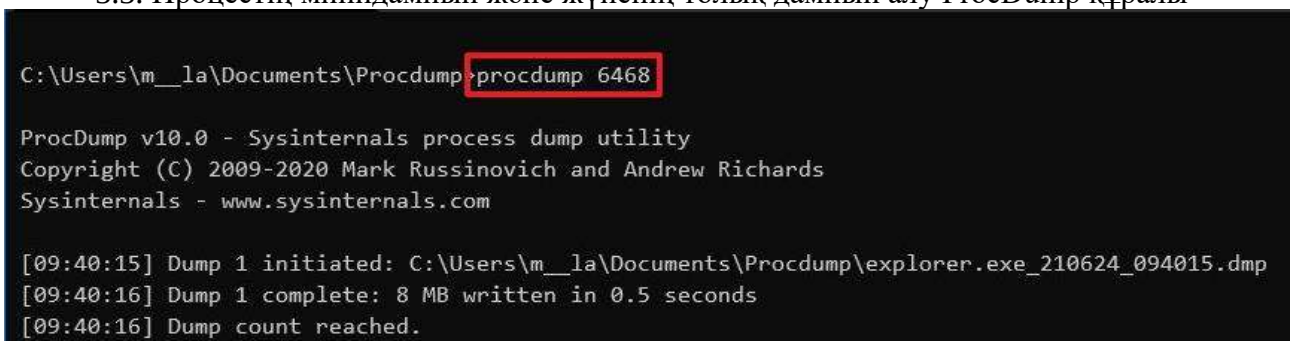
LiME (Linux Memory Extractor) Linux жүйесінде жадты толық бейнелеу жасауға мүмкіндік беретін ашық кодты құрал. Ол жадтың барлық мәліметтерін шығаруға және сақтауға арналған, әсіресе қауіпсіздік инциденттері мен қылмыстық тергеулерде пайдалы. LiME жадтағы процестердің, жүйелік ақпараттардың және бағдарламалық деректердің толық көшірмесін сақтай алады. Бұл құрал цифрлық криминалистикада жүйенің күйін зерттеу үшін қолданылады, сонымен қатар зиянды бағдарламаларды анықтауға көмектеседі. LiME жадты RAW және EWF форматтарында сақтай алады, бұл зерттеулер үшін ыңғайлы болып табылады. Ол Linux жүйесінің түрлі архитектураларын қолдайды, соның ішінде ARM және x86. LiME жүйені зерттеу кезінде нақты ақпаратты алу үшін қажетті құрал болып табылады.

3.2. Процесс дампын алу gcore құралы

Сурет 2. Процесс дампын қолға түсіру барысы.

gcore Linux жүйесінде жұмыс істеп тұрған процестің жадын жедел түрде түсіріп алуға мүмкіндік беретін құрал. Ол белгілі бір процестің жадын толық немесе ішінара көшіру арқылы, оның күйін сақтап, кейіннен талдауға мүмкіндік береді. gcore процесстің жадын core dump файлы ретінде сақтайды, бұл деректер қателіктерді немесе өнімділік мәселелерін зерттеуге пайдалы болады. Бұл құрал әсіресе бағдарламалық қателерді, құлауларды немесе өнімділік ақауларын анықтау кезінде қолданылады. Ол жұмыс істеп тұрған процестердің күйін терең зерттеуге мүмкіндік береді, бұл тергеу немесе талдау үшін маңызды болуы мүмкін. gcore процесстің барлық жадын, оның ішінде ішкі деректер мен айнымалыларды сақтайды, бұл бағдарламаның нақты күйін көрсетуге көмектеседі. Бұл құрал жүйенің ақауларын немесе қосымшаның қатесін табу үшін тиімді қолданылады. Сонымен қатар, gcore басқа процестерге әсер етпей, тек бір процестің жадын түсіруге мүмкіндік береді. Алынған мәліметтер кейінірек аналитикалық құралдармен талданып, қателіктер мен өнімділік мәселелері анықталады. gcore жалпы түрде жүйелік мониторинг пен қателіктерді түзету үшін кеңінен қолданылатын құралы болып табылады..

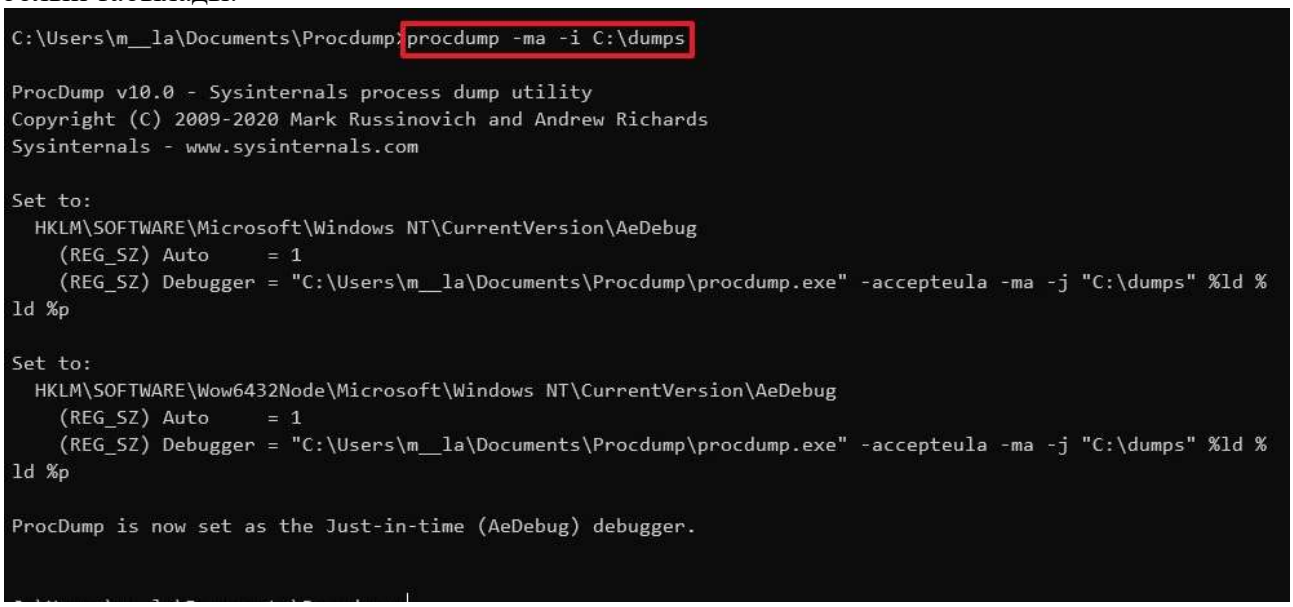
3.3. Процестің минидампын және жүйенің толық дампын алу ProcDump құралы



Сурет 3. Белгілі бір процесстің минидампын қолға түсіру барысы.

ProcDump Windows жүйесінде процестердің жадын түсіру және оларды талдау үшін қолданылатын құрал. Ол процестердің жадын core dump түрінде сақтап, жүйелік ақауларды, бағдарлама қателіктерін немесе өнімділік мәселелерін анықтауға көмектеседі. ProcDump құралын әсіресе жүйе қателіктері немесе апаттық жағдайларды тергеу кезінде қолдануға болады. Бұл құрал нақты уақытта жұмыс істеп тұрған процестердің жадын түсіріп, кейіннен талдауға мүмкіндік береді. ProcDump егер процесс белгіленген шарттарға сәйкес тоқтап немесе қателессе, жадты автоматты түрде түсіре алады. Ол сондай-ақ, процесс тұрақты түрде жауап бермеген кезде немесе басқа белгілі бір шарттар орындалғанда dump файлдарын жасауға арналған. ProcDump алынған жад файлдарын түрлі дебаггерлермен немесе талдау құралдарымен тексеруге мүмкіндік береді. Оның қолданылуы жүйелік қауіпсіздікті

қамтамасыз ету және бағдарламалық ақауларды түзету мақсатында кеңінен таралған. ProcDump — ақауларды анықтау және жүйелік қателіктерді түсіну үшін аса маңызды құрал болып табылады.



Сурет 4. Жүйенің толық дампын алу.

ProcDump құралын қолдана отырып, толық жадтың дампын алу үшін алдымен процесс идентификаторын (PID) анықтау қажет. Бұл үшін Task Manager немесе командалық жол арқылы процесті табуға болады. Процесстің толық жадын алу үшін -ma параметрін пайдалану керек, ол процесс туралы барлық ақпаратты, соның ішінде барлық айнымалылар мен буферлерді сақтайды. Бұл үшін 4-суретке назар аударсақ болады. Бұл команда процесстің барлық жадын, оның ішінде ядро деңгейіндегі ақпаратты да қамти отырып, көрсетілген файлға сақтайды. Алынған дамп файлы кейінірек қателіктерді немесе өнімділік мәселелерін тергеу үшін талданады. ProcDump жадтың толық көшірмесін алу кезінде жүйені ешқандай қиындыққа ұшыратпайды, себебі ол тек бір процесті ғана зерттейді. Осылайша, құралдың көмегімен жадыдағы маңызды деректерді сақтап, олардың күйін кейінірек толық зерттеуге болады.

4. Дамп түрлерін алуды салыстыру

Дамп түрлерін салыстыру кестесін деректер көлемі, жасалу уақыты, талдау мүмкіндігі және қолдану мысалы критерийлері бойынша жүйелеуге болады.

Критерий	Толық дамп	Ядро дампы	Минидамп	Процесс дампы
Деректер көлемі	100% RAM	30–50% RAM	<2 МБ	Процесске байланысты
Жасалу уақыты	Ұзақ	Орташа	Қас-қағым	Жылдам
Талдау	Максималды толық	Драйверлер/ядро	Негізгі	Белгілі процесс
Қолдану мысалы	Криминалистика	BSOD талдауы	Жылдам диагностика	Бағдарлама отладкасы

Кесте 2. Дамп түрлерінің салыстыру кестесі

Қорытынды

Жады дамптарын кескінін алу құралдары жүйелердің тұрақтылығы мен қауіпсіздігін қамтамасыз ету үшін өте маңызды рөл атқарады. Бұл құралдар бағдарламалық қателіктерді, жүйелік ақауларды, өнімділік мәселелерін анықтауға және тергеуге мүмкіндік береді. Толық дамптар, мысалы, WinDbg және LiME, күрделі жүйелік ақауларды терең зерттеу үшін

алмастырылмайды, себебі олар жүйенің барлық ақпаратын қамтып, қателіктер мен ақауларды егжей-тегжейлі талдауға мүмкіндік береді. Ядро дамптары, мысалы, kdump және WinDbg, драйверлер мен BSOD (Blue Screen of Death) диагностикасы үшін өте тиімді, себебі олар тек жүйенің ядросындағы қателіктерді анықтауға бағытталған. Қосымшаларды жылдам отладкалау және ақауларды тез анықтау үшін ProcDump және gcore сияқты процесс дамптары қолайлы, өйткені олар тек белгілі бір процестердің күйін талдауға мүмкіндік береді. Минидамптар, мысалы, Windows WER және systemd-coredump, бастапқы талдау жасауға арналған, себебі олар толық дамптарға қарағанда аз көлемде ақпарат сақтайды, бірақ жүйедегі маңызды қателіктерді анықтауға болады. macOS жүйесінде osxpmem және lldb сияқты құралдар жадының толық және егжей-тегжейлі талдауын қамтамасыз етеді. Ал Volatility криминалистика саласында әмбебап құрал ретінде кеңінен қолданылып, әртүрлі платформаларда жадты талдауға мүмкіндік береді. Жады дамптарын жасау құралының таңдауы нақты міндетке байланысты: жүйелік ақауларды тергеу үшін WinDbg және crash жақсы таңдау болса, процестердің жұмысын талдау үшін ProcDump және gcore қолданылады. Linux және macOS жүйелерінде толық талдау үшін LiME және osxpmem сияқты құралдар пайдаланылса, Windows жүйесінде дамптарды жасау үшін WinDbg және басқа да арнайы құралдар қолданылады. Құралдарды дұрыс таңдау жүйедегі қателіктерді анықтап, жоюға, сонымен қатар жүйелік қауіпсіздікті сақтауға көмектеседі. Бұл құралдардың барлығы тергеу, отладка және қауіпсіздік саласындағы маңызды аспектілерді қамтамасыз етеді, оларсыз күрделі мәселелерді шешу мүмкін болмас еді.

Қолданылған әдебиеттер тізімі

1. Русинович М., Соломон Д., Ионеску А. Windows Internals, Part 1. - 7th ed. - Microsoft Press, 2021. - 832 с.
2. Ligh M., Case A., Levy J. The Art of Memory Forensics. - Wiley, 2014. - 912 с.
3. Карпенко А.Б., Шакин В.Н. Анализ дампов памяти в цифровой криминалистике. - М.: ДМК Пресс, 2021. - 342 с.
4. Скляров Д.В. Современные методы анализа оперативной памяти. - СПб.: БХВ-Петербург, 2022. - 415 с.

ЕКІ ФАКТОРЛЫ АУТЕНТИФИКАЦИЯНЫҢ ҚАУІПСІЗДІГІ ЖӘНЕ ОНЫҢ ҚОЛДАНЫЛУЫ

Жолмұратұлы Б., Маратов Ә.Б., Ховдабай Н.А.
[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
Астана, Қазақстан.
Nurjigitkhovdabai@gmail.com,alih.marat.05@gmail.com
Ғылыми жетекші – Қазиева Н.М.

Аннотация

Бұл мақалада екі факторлы аутентификацияның (2FA) қауіпсіздігі қарастырылады және оның басқа аутентификация әдістерімен салыстырмалы талдауы жүргізіледі. Қазіргі таңда ақпараттық қауіпсіздіктің маңыздылығы арта түсуде, сондықтан пайдаланушылардың деректерін қорғау әдістері үздіксіз дамып келеді. 2FA – пайдаланушының жеке басын қосымша растау әдісі арқылы аутентификациялау технологиясы. Мақалада 2FA-ның тиімділігі, оның артықшылықтары мен кемшіліктері қарастырылады.

Кілттік сөздер: екі факторлы аутентификация (2FA), ақпараттық қауіпсіздік, киберқауіпсіздік, SMS-код, парольдік қауіпсіздік.