ӘОЖ 004.056.5

ПЕНТЕСТИНГ – АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ АРТТЫРУ ҚҰРАЛЫ: ӘДІСТЕМЕ ЖӘНЕ ТӘЖІРИБЕ

Эркинова Нуриза Алишеровна
nurerkinova11@gmail.com
6В06114 «Информатика және ақпарттық- коммуникациялық технологиялар»
білім беру бағдарламасының 3 курс студенті
Цой Александр Константинович
coisasha25@gmail.com,
6В06113 «Бағдарламалау және бағдарламалық қамтамасыздандыруды әзірлеу»
білім беру бағдарламасының 3 курс студенті
М.Х.Дулати атындағы Тараз университеті, Тараз қаласы, Қазақстан Республикасы
Ғылыми жетекші – **Р.Н. Тажиева,** аға оқытушы
tazhieva1978@mail.ru

Аннотация

Бұл зерттеу жұмысы пентестингтің тарихын, ақпараттық қауіпсіздікті арттырудағы рөлін, әдістемелерін және тәжірибелік қолдануын қарастырады. Пентестинг – ақпараттық жүйелер мен желілердің қауіпсіздігін тексеру мақсатында жүргізілетін,әлсіз тұстарды табу үшін арнайы жасалатын тестілеу процесі. Жұмыста пентестингтің негізгі кезеңдері, құралдары және тәсілдері талданады. Негізігі мақсаттары: Қауіпсіздіктің әлсіз тұстарын табу, шабуылдарға төтеп беру қабілетін тексеру, рұқсатсыз кіру мүмкіндігін анықтау болып табылады. Теориялық шолу негізінде қазіргі заманғы әдістемелер сипатталып, тәжірибелік мысалдар келтіріледі. Сонымен қатар, пентестингті криптография саласында қарастырамыз, оның ішінде Цезарь, Вижинер әдістерімен біріктіреміз.

Негізгі сөздер: Ақпарат жинау, осалдықтарды анықтау, эксплуатация, сұр жәшік, қара жәшік, ақ жәшік, DDoS шабуылдар, фишинг, Nmap, Zenmap,VPN, хакерлік шабуылдар, екі деңгейлі аутентификация, SQL Injection, Цезарь, Вижинер,HashCalc.

Қазіргі заманғы цифрлық технологиялардың қарқынды дамуы ақпараттық қауіпсіздік мәселелерін өзекті етуде. Кибершабуылдар мен деректердің бұзылу қаупінің артуы ұйымдардың ақпараттық жүйелерін қорғау қажеттілігін күшейтті. Осы тұрғыда пентестинг – қауіпсіздік деңгейін бағалаудың және осалдықтарды анықтаудың маңызды әдістерінің бірі болып табылады. Пентестингтің негізігі құралы Metasploit, Nmap, Wireshark, Burp Suite және John the Ripper. Metasploit – ең танымал эксплуатациялық платфома болғандықтан шабуыл модельдеуге және осалдықтарды сынауға арналған.

Metasploit бастапқыда HD Moore жасаған және ойластырған қауіпсіздік фирмасында жұмыс істеді. HD не жұмсайтынын түсінген кезде уақытының көп бөлігін қоғамдық эксплуатация кодын тексеру және тазарту үшін ол бастады жасау үшін икемді және техникалық қызмет көрсетуге ыңғайлы платформа жасаңыз және эксплуатацияларды әзірлеу.

Ол Perl негізіндегі алғашқы Metasploit басылымын шығарды 2003 жылдың қазан айында барлығы 11 эксплуатация жасалды. Spoonm көмегімен HD жобаның толық қайта өңделген нұсқасын шығарды, Metasploit 2.0 2004 жылдың сәуірінде. Бұл нұсқада 19 эксплуатация және 27-ден астам эксплуатация болды пайдалы жүктемелер. Осы шығарылым шыққаннан кейін көп ұзамай Мэтт Миллер (Skape) Metasploit әзірлеушілер тобына қосылды жоба танымал бола бастаған кезде Metasploit платформасы ақпараттық қауіпсіздік қоғамдастығының кең қолдауына ие болды және ол тез ену және пайдалану сынағы үшін қажетті құралға айналды [1].

Nmap – желіні сканерлеуге және ашық порттарды анықтауға арналған құрал. IP-мекенжайларды, хосттарды және желілік құрылғыларды анықтайды. Ашық және жабық порттарды табады, олардың қауіпсіздігін бағалайды. Қандай протоколдар мен қызметтер мысалы, HTTP, SSH, FTP белсенді екенін көрсетеді.

Wireshark – желілік трафикті талдауға арналған ашық кодты бағдарлама. Ол пакеттерді ұстап алып, олардың мазмұнын егжей-тегжейлі талдауға мүмкіндік береді. Wireshark желінің жұмысын тексеру және мәселелерді диагностикалауда, шабуылдарды талдау, зиянды әрекеттерді анықтауда, қосымшаларды әзірлеу және тестілеуде және студенттер мен мамандарға желілік хаттамаларды оқып-үйрену үшін қолданылады.

Пентестер – ақпарттық қауіпсіздік саласындағы маман, ол жүйелердің осал тұстарын анықтау үшін оларды әдейі бұзуға тырысады. Пентестер IT-инфрамқұрылымына хакерлік шабуыл жасау арқылы оның қорғалу деңгейін тексереді. Әртүрлі әдістерді қолдану SQL Injection, XSS, фишинг, эксплойттар және т.б. арқылы жүзеге асырады.

Әлсіз және әлсіз жақтарын анықтаудың ең тиімді әдістерінің бірі- олар бұзуды бастамас бұрын, қауіпсіздік-бұл кәсіби маманды жалдау- модельдеуге арналған кәсіби "зұлым" немесе пенестер- компанияның инфрақұрылымына шабуыл. Пенестер қабылдауы керек шынайы әрекетке еліктеу үшін барлық қол жетімді әрекеттер шабуылдаушы- ника кейбір жағдайларда толық құпиялылық жағдайында әрекет етеді, ішкі қауіпсіздік бөлімі мен қызметі үшін соңғы есебіңізді жариялау уақыты келгенше. Бұл кітапта мен шабуыл әрекетінің бұл түрін келесідей атаймын тек ену сынағы арқылы қауіпсіздікті қамтамасыз ету [2].

John the Ripper – бұл парольдерді бұзу және қауіпсіздік тексерулерін жүргізуге арналған ашық кодты құрал. Негізгі мүмкіндіктері: хэштерді бұзу – MD5, SHA-1,SHA-256, NTLM және басқа хэш алгортитмдерді қолдайды.

SQL-инъекция – бұл веб-қосымшаның дерекқорымен өзара әрекеттесу тәсілін бұзу арқылы орындалатын хакерлік шабуыл түрі.

SQL инъекциясы (Sql) вебке шабуыл жасау үшін piggyback SQL командаларына шабуыл жасайды қауіпті кодты қолданатын қолданбалар. SQL сұрауын енгізуге болады деректер базасында командаларды орындау үшін сенімді веб-сервер арқылы ішкі мәліметтер базасы. Fast-Track кеңейтілген SQL енгізу процесін автоматтандырады Fast-Track 165 сұрау жолын және вебтегі POST опцияларын қолданатын шабуылдар қосымшалар. Келесі шабуыл шабуылдаушының SQL енгізу екенін білуіне негізделген мақсатты веб-сайтта бар, сонымен қатар қай опция ең осал екенін біледі қабілетті. Бұл шабуыл тек MS SQL негізіндегі жүйелерде жұмыс істейді [3].

Киберқауіпсіздік саласында ең көп таралған шабуылдардың бірі – DDoS және фишинг. Бұл шабуылдар ұйымдар мен жеке тұлғаларға айтарлықтай зиян келтіріп, олардың жүйелерін, желілерін және жеке ақпараттарын қауіпке ұшыратады. Фишингтен қорғану жолдары:электрондық хаттардағы сілтемелерге сақтықпен қарау. Жеке ақпаратты ешқашан электрондық пошта немесе телефон арқылы жібермеу. Антивирус және фишингке қарсы құралдарды пайдалану. Құпиясөзді екі факторлы аутентификация (2FA) арқылы қорғау. HTTPS протоколы бар ресми веб-сайттарды ғана қолдану.

Екі деңгейлі аутентификация (2FA) – пайдаланушының жүйеге кіруін растау үшін екі түрлі қауіпсіздік факторы қолданылатын аутентификация әдісі. Бұл құпиясөз бұзылған жағдайда да есептік жазбаны қорғауға көмектеседі. Екі деңгейлі аутентификация – аккаунттарды қорғаудың тиімді тәсілдерінің бірі. Ол кибершабуылдардың көпшілігін

болдырмауға көмектеседі және жеке мәліметтерді қауіпсіз сақтауға мүмкіндік береді. Барлық маңызды есептік жазбаларда 2FA қолдану – қауіпсіздік мәдениетінің негізгі бөлігі.

Пентестингте Вижинер шифрын біріктіру арқылы деректерді қорғау немесе керісінше, осалдықтарды анықтау әдістерін зерттеуге болады. Бұл шифр да симметриялық криптографияның қарапайым түрі болғанымен, оның комбинациясы қызықты зерттеу тақырыбы бола алады.

Виженер әдісі көпалфавитті алмастыру формасындағы қарапайым әдіс болып табылады. Виженер шифры көптеген өңдеулерден кейін қолданыс тапты. Алғаш рет бұл әдіс Джованни Бастисто Беллазо (Giovan Battista Bellaso) авторының La cifra del кітабында жарық көрген. 19 ғасырдың 1553 жылы Sig. Giovan Battista Bellasoy швецариялық дипломат Блез Виженердің атымен аталды. Бұл әдіс криптоталдау жасауға оңтайландырылған әрі түсіндіру мен қолдануға тиімдірек [4].

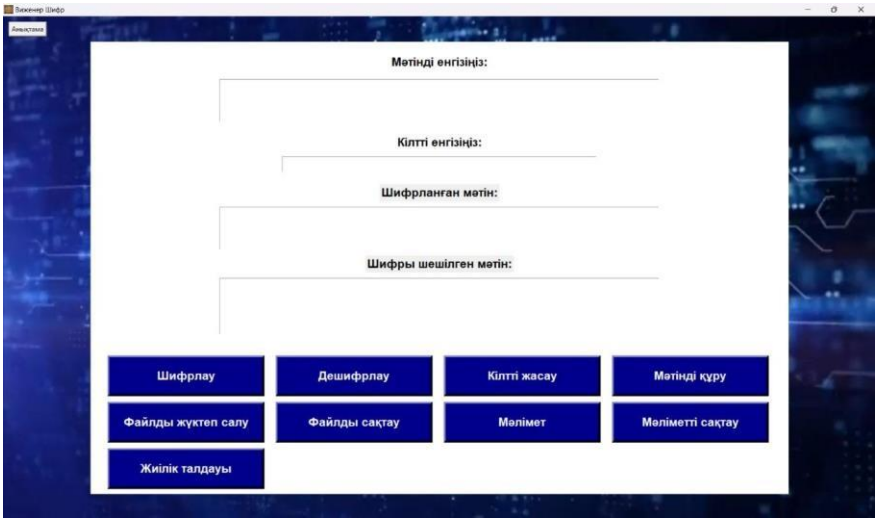
Visual Studio-да жасалған бағдарлама мәтіндік деректерді қорғау үшін қолданылатын Виженер шифрлау алгоритмін жүзеге асыруға арналған. Ол пайдаланушыларға берілген кілтті пайдаланып мәтінді шифрлау мен шифрды шешуге мүмкіндік беретін ыңғайлы графикалық интерфейсті ұсынады

Бағдарламаның негізгі мүмкіндіктері:

1. Мәтін мен кілтті енгізу:

Пайдаланушы берілген мәтінді арнайы берілген өріске өңдеу үшін енгізеді.

Шифрлау немесе шифрды анықтау үшін қажетті кілт жеке өріске енгізіледі. Ол деректердің қауіпсіздігін қамтамасыз етуде маңызды рөл атқарады. Бағдарламаның басты терезесі 1-суретте келтірілген.

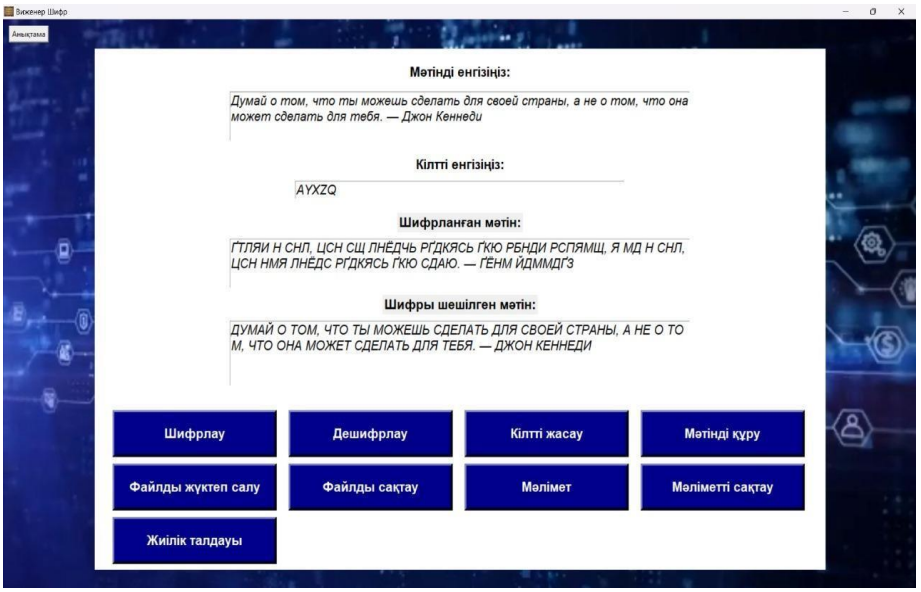


Сурет 1 – Бағдарламаның басты терезесі

2. Өңдеу нәтижелері:

Шифрланған мәтін шифрлау операциясын орындағаннан кейін арнайы терезеде көрсетіледі. Транскрипцияланған мәтін өрісі шифрды шешкеннен кейін бастапқы мәтінді көрсетеді.

3. Басқару түймелері мен олардың атқаратын функциялары: «Шифрлау» – мәтінді кілт негізінде түрлендіру процесін орындайды. «Дешифрлау» - шифрланған мәтінді бастапқы көрінісіне қайтарады. «Кілтті жасау» – шифрлауға арналған кілтті автоматты түрде жасайды. «Мәтінді құру» – одан әрі өңдеу үшін мәтінді енгізеді. «Жиілік талдауы» – шифрланған мәтіндегі таңбалардың жиілігін талдайды. Осы басқару түймелері арқылы орындалған шифрлау нәтижесі 2-суретте көрсетілген.

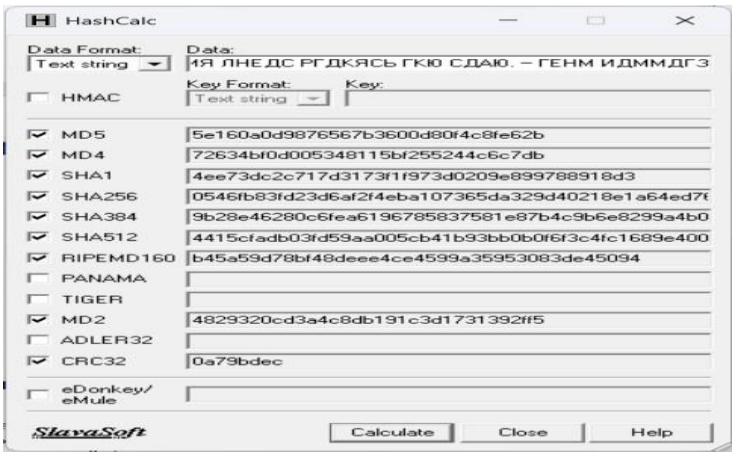


Сурет 2 – Бағдарламаның орындалу нәтижесі

4. Файлдармен жұмыс істеуге арналған батырмалардың функциялары: Пайдаланушы мәтіндік файлды "Файлды жүктеп алу" батырмасы арқылы жүктей алады. Өңделген деректерді сақтау "Файлды сақтау" батырмасы арқылы жүзеге асырылады.

5. Қосымша ақпараттар алуға болатын батырмалар:

"Мәлімет" бөлімі бағдарлама және оның функциялары туралы анықтамалық ақпарат береді. "Мәліметті сақтау" опциясы бағдарламаның шығуын файл түрінде сақтауға мүмкіндік береді.



Сурет 3 – Вижинердегі щифрланған мәтәнді хэштеу

Енді біз бұл жерде Вижинер шифрын қолданып, нәтижесінде алынған шифрланған мәтінді HashCalc көмегімен хэштей аламыз 3-суретте көрсетілген. Вижинер шифрымен шифрланған мәтінді хэштеу арқылы оның тұтастығын тексеруге болады. Егер кілт белгісіз болса, брутфорс (толық тексеру) немесе сөздік шабуылы (dictionary attack) арқылы дұрыс кілтті табу үшін хэшті қолдануға болады. Болжамды кілтпен Вижинер шифрын шешіп көру. Шыққан мәтіннің хэшін есептеу. Егер ол белгілі бір эталондық хэшпен сәйкес келсе, кілт дұрыс.

Қорытындылай келе, ақпараттық қауіпсіздік – үнемі дамып отыратын сала. Жаңа осалдықтар мен шабуыл әдістері пайда болған сайын, оларға қарсы қорғаныс құралдары да жетілдірілуде. SQL-инъекция, пентестинг, желілік қауіпсіздік және парольдерді қорғау сияқты аспектілер өзара тығыз байланысты және кешенді түрде қарастырылуы тиіс. Кибершабуылдардың алдын алу үшін қауіпсіздік жүйесін тұрақты түрде тексеріп отыру, осал

тұстарды дер кезінде анықтау, тиімді қорғаныс шараларын енгізу және ақпараттық қауіпсіздік мәдениетін қалыптастыру маңызды. Тек осындай кешенді тәсіл арқылы жеке мәліметтер мен корпоративтік желілердің қауіпсіздігін қамтамасыз етуге болады.

Виженер алгоритмін практикалық зерттеуге де, құпия мәтіндік деректерді қорғауға да жарамды. Сондай-ақ, бағдарламаны жиілік криптоаналитикасын талдау үшін білім беру мақсатында пайдалануға болады. HashCalc арқылы Вижинер шифрланған мәтіннің өзгермегенін тексеруге болады. Вижинер кілтін хэштеу арқылы оны қауіпсіз сақтау мүмкіндігі бар. Хэш арқылы Вижинер шифрын бұзу және дұрыс кілтті табу оңайырақ болады.

Қолданылған әдебиеттер тізімі:

1. Дэвид Кеннеди, Джим О ' Горман, Девон Кернс және Мати Аарони METASPLOIT The Penetration Tester’s Guide [Электрондық ресурс] авторлық құқық 2011.-22 бет
2. Дэвис Р. Искусство тестирования на проникновение в сеть / пер. с анг. В. С. Яценкова. – М.: ДМК Пресс, 2021. – 25 с.: ил.
3. Дэвид Кеннеди, Джим О ' Горман, Девон Кернс және Мати Аарони METASPLOIT The Penetration Tester’s Guide [Электрондық ресурс] авторлық құқық 2011.-164-165 бет
4. Якубов, Б.М. Телекоммуникациялық жүйелердегі ақпараттар қауіпсіздігі [Электрондық ресурс]: Оқу құралы / Б. М. Якубов, А. К. Мекебаева, 2017. – 82 б.