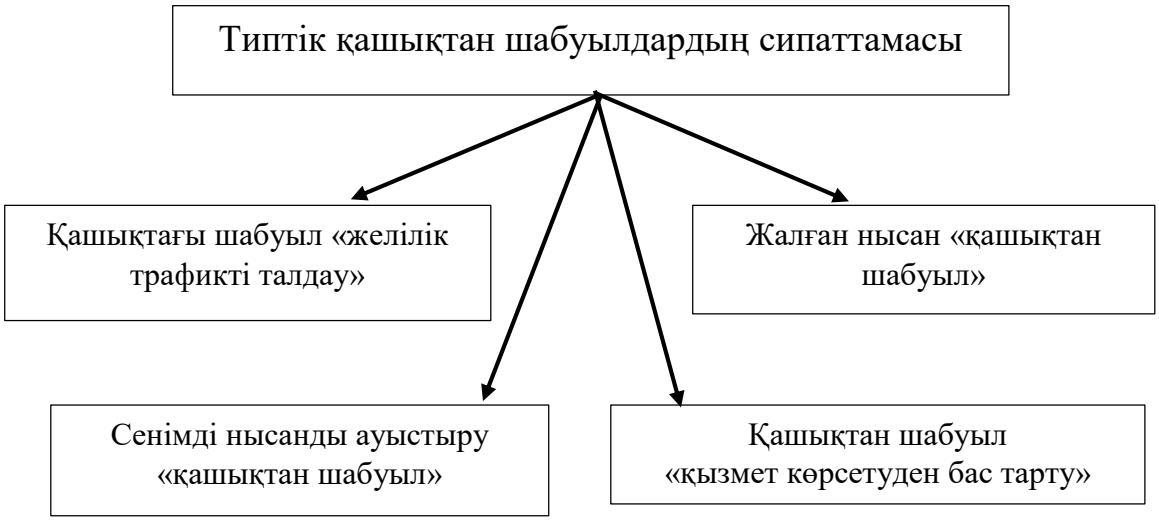
Дәріс №3. Осал желілік хаттамаларға негізделген типтік шабуылдар механизмдері

1) Қашықтықтан шабуыл ұғымы;
2) Осал желілік хаттамаларға негізделген типтік шабуылдар механизмдері

1) Қашықтықтан шабуыл ұғымы

Қашықтан шабуыл - бұл байланыс арналары арқылы бағдарламалық түрде жүзеге асырылатын және кез-келген таратылған компьютерлік желіге тән қашықтықтан ақпараттық деструктивті әсер.



1- сурет. Типтік қашықтан шабуылдардың сипаттамасы

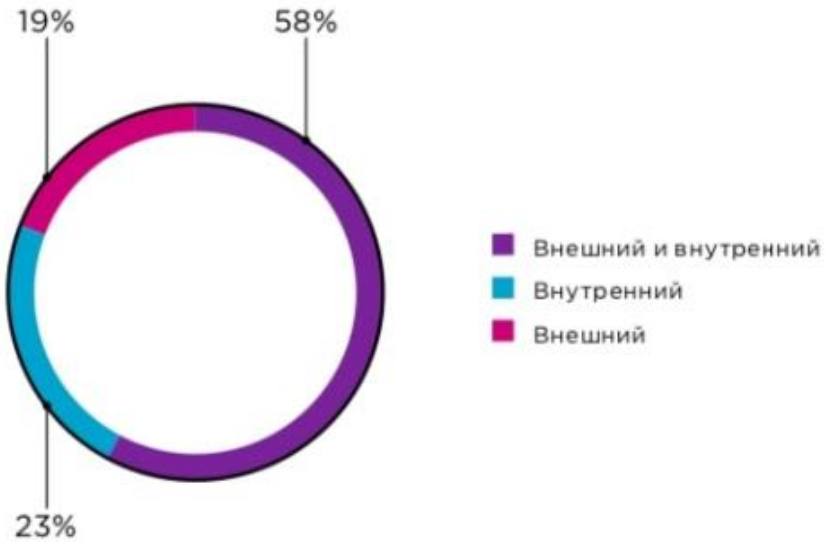
Таратылған компьютерлік желінің басты ерекшелігі - оның объектілерінің кеңістіктегі таралуы және олардың арасындағы физикалық байланыс желілері арқылы байланыс. Бұл ретте есептеу желісі объектілері арасында жіберілетін барлық басқарушы хабарламалар мен деректер алмасу пакеттері түрінде желілік қосылыстар бойынша беріледі. Бұл мүмкіндік желілік трафикті талдау деп аталатын байланыс арнасын тыңдаудан тұратын таратылған компьютерлік желілерге тән типтік қашықтан әсер етті.

Ену тестілеуі (*Тестирование на проникновение*)-бұл этикалық хакерлер деп аталатын нақты зиянкестердің әрекеттерін модельдеу. Көбінесе бұл термин қысқартылып, мұндай жұмыстарды **пентест** деп атайды, ал оларды жүргізетін сарапшылар **пентестер**. Пентест аясында АҚ мамандары белгілі бір компанияның жүйелеріндегі осалдықтарды іздейді және белгіленген қорғаныс құралдарын айналып өтіп шабуыл жасауға тырысады.

Тестілеу сыртқы желілерден (мысалы, интернеттен) жасалған кезде, **пентест сыртқы** деп аталады. Егер компания ішіндегі құқық бұзушының шабуылдары

модельденсе (мысалы, қызметкер артықшылықтарының типтік жиынтығымен немесе кездейсоқ келуші атынан), онда пентест әдетте ішкі деп аталады.

Соңғы уақытта компаниялар сыртқы және ішкі пентестті жүргізген күрделі жобалар үлесінің арту үрдісі байқалады. Сонымен қатар, ішкі пентест сыртқы жағдайдың жалғасы болуы мүмкін: бұл тәсіл шабуылдаушының жергілікті желіге ену ықтималдығын ғана емес, сонымен қатар компанияның инфрақұрылымындағы шабуылдың салдарын да бағалауға мүмкіндік береді.



*2 – сурет. Positive Technologies компаниясыны 2019ж. талдау*ы

Енуге тестілеудің мақсаты - пайдаланылатын қорғау жүйелерінің тиімділігін және компанияның ақпараттық инфрақұрылымының жалпы кибершабуылдарға дайындығын бағалау. Пентест аясында, егер басшылық оларды жүргізіліп жатқан жұмыстар туралы хабардар етпесе, компанияның АҚ қызметтерінің анықтау мен жолын кесудегі тиімділігін бағалауға болады.

Пентест *осалдықтарды анықтауға бағытталған* деп ойлау қате; бұл негізгі міндет емес. Хакерлер қауіпсіздіктің кемшіліктерін іздейді - бірақ оларды тек пентест мақсаттарына жету үшін пайдалану керек. Мысалы, *сыртқы тестілеу жағдайында* міндет, әдетте, ұйымның жергілікті желісіне кірудің максималды санын анықтау болып табылады; *Ішкі жағдайда* — шабуылдаушы ала алатын артықшылықтардың максималды деңгейін анықтау. Пентесттің тұтынушысы басқа міндеттерді қосымша қоя алады (мысалы, нақты бизнес жүйелеріне қол жеткізу мүмкіндігін көрсету).

2) Осал желілік хаттамаларға негізделген типтік шабуылдар механизмдері

Сайтты бұзу— бұл зиянкестің сайттың файлдарына немесе сайтты басқару жүйесін әкімшілендіру бөліміне рұқсатсыз қол жеткізуі.

Бұзулардың екі түрі болады:

Мақсатты — мұндай жағдайда зиянкес нақты бір сайтты бұзуды міндетіне алады, мәселен, сайтқа кірушілердің немесе иесінің құпия деректеріне қол жеткізу үшін. Бұзудың бұл түрі сирек кездеседі және одан әрі қаралмайды, алайда оған қарсы іс-қимыл жасау үшін жалпы бұзуға қарсы іс-қимыл жасауда пайдаланылатын құралдар қолданылады.

Жалпы — бұл жағдайда нақты бір сайт маңызды болмайды. Зиянкес алдағы уақытта өз мақсаттарында пайдалану үшін еркін сайттардың барынша көп санына қол жеткізуге тырысады. Баяндалатын тақырып бұзудың осы түрі туралы.

Бұзудың нәтижесінде зиянкес сайтқа еркін файлдарды жүктей алады, скриптерді енгізе алады, сайттың мазмұнын өзгерте алады, сондай-ақ сайт кірушілермен алмасатын деректерді ұстап қалу мүмкіндігі болады. Зиянкес сайтты бұзып, біріншіден, бұзылған сайт шегінде кез келген скрипттерді орындау мен кез келген ақпаратты орналастыру үшін немесе спам таратуға арналған тегін және анонимді хостинг алады, ал екіншіден, ол сайтқа кірушілерге қол жеткізе алады және сайттың парақтарынан кірушілердің компьютерлерін зақымдайды немесе оларды зиянды сайттарға бағыттай алады.

Сонымен қатар бұзылған сайттар DDoS шабуылдарды, басқа сайттарды бұзуды жүзеге асыру мен басқа кез келген зиянды бағдарламаларды іске қосу үшін пайдаланылады, себебі сайт орналасатын хостинг аккаунты – бұл хостинг серверіндегі операциялық жүйенің кез келген қосымшаларды іске қосуға мүмкіндік беретін толық пайдаланушылық аккаунты.

Зиянкес сайтты бұзу үшін оған сайттың файлдарын өзгертуге мүмкіндік беретін кез келген әдісті қолдануы мүмкін.

Бұзудың ең жиі кездесетін әдістері:

1. Сайттың иесі немесе әзірлеуші **FTP** арқылы сайтқа қосылатын компьютердегі вирустың көмегімен зиянкес **FTP аккаунтының паролін ұрлайды, содан кейін аккаунтқа қосылып,** еркін файлдарды өзгерте немесе жүктей алады. Сайт атауы сайттың атауына ұқсас папкада жиі орналастырылатыны себепті зиянкес ол бұзып енген сайтты тез анықтайды. Сондай-ақ сайттың атауы туралы ақпарат зиянкес ұрлаған FTP-ны іске қосудың күйге келтірулерінде жиі орналастырылады.

2. FTP бойынша қол жеткізуге ұқсас **ұрланған SSH бойынша қол жеткізу әдісі де қолданылады. Бірақ одан ерекшелігі еркін бағдарламаларды іске қосу үшін SSH** бойынша жұмыс істеу кезінде аккаунтта орналасқан сайтты пайдалану талап етілмейді.

3. Сонымен қатар зиянкес сайттың парақтарын редакциялауға арналған **оның әкімшілендіру панелінің паролін ұрлай алады.** Әдетте, әкімшілендіру панелі сайтқа еркін файлдарды жүктеуге мүмкіндіктер береді. Зиянкес оны пайдалана отырып, сайтқа зиянды скрипт жүктейді және ол арқылы әкімшілендіру панеліне кіру қажеттілігісіз сайтпен одан әрі жұмыс істеуді жүзеге асырады.

4. FTP, SSH немесе сайттың әкімшілендіру панелінің паролін зиянкес **пароль айтарлықтай күрделі болмаса,** сөздік бойынша теру арқылы біле алады.

5. Зиянкес парольді пайдаланбай **сайтты басқару жүйесінде (CMS) немесе оның кеңейтулерінің беруінде қолданылатын осалдық арқылы** сайтқа кіре алады. Мұндай жағдайда зиянкес бағдарламаның логикасындағы қатені пайдаланады және жүйені оны әзірлеуші көздеген қалыпта жұмыс істеуге мәжбүрлейді. Осы іс-қимылдардың нәтижесінде зиянкес сайтқа жұмысты одан әрі жалғастыруға арналған скриптті жүктей алады. Қандай да бір CMS қатысты қандай болсын осалдық қалай қолданылатынын білгісі келген кез келген адамға көмектесетін осалдықтар қоры болады. Бұзудың бұл әдісі өте жиі қолданылады, себебі осалдықтар қоры CMS-тегі жаңа қателер туралы хабарламалармен үнемі толықтырылады, ал сайттардың иеленушілері сайтты немесе олардың кеңейтулерін басқару жүйесін осалдықтарға ұшырамайтын өзекті нұсқаларына дейін сирек жаңартады.

6. Сайтқа кіргеннен кейін зиянкес ол арқылы хостингтің сол аккаунтында орналасқан басқа сайттарға да қол жеткізе алады. Демек, сайтта осалдықтар болмаған және FTP немесе SSH бойынша оған қол жеткізу мүмкін болмаса да – **осал сайтпен бір аккаунтта орналасқанына** байланысты сайт бұзылуы мүмкін.

Сайтты қандай да бір әдіспен бұзғаннан кейін зиянкес, көптеген жағдайларда, оған **осалдық жабылған, ал барлық парольдер өзгертілген болса да** сайтқа алдағы уақытта кіруге мүмкіндік беретін бір немесе бірнеше скрипт жүктейді. Әдетте, зиянкес мұндай скрипттерді сайт папкаларының құрылымына терең орнатып немесе CMS скрипттеріне ұқсас атаулармен оларды жасыруға тырысады. Сонымен қатар басып енуге арналған код CMS қолданыстағы файлдарының біреуіне енгізілуі мүмкін – осылайша зиянкес зиянды кодты айқындауды қиындатып, жаңа файлдар құрудан аулақ болады.

Зиянкестің мақсаты нақты бір сайтты емес, барынша көп сайтты зақымдау болатыны себепті ол түгелдей барлық сайттарға қол жеткізуге тырысады. Іріктеу үшін сайттардың тізімін алуға іздестіру жүйесін пайдалану жеткілікті болады. Егер қандай да бір сайт бұзылса, бұған зиянкес кенеттен оны іздестіру жүйесінен немесе атауларын теру арқылы тауып алғанына және сайтта осалдықтың орын алуына байланысты, не сайтқа қол жеткізу парольдері жария етілгені себепті жол беріледі.

Осымен, «ол туралы ешкім білмейді» деген себеппен сайтқа қауіп төнбейді деп ойлауға болмайды. **Сайттың қауіпсіздігін** қамтамасыз ету үшін мына шараларды қолдану қажет:

CMS және оның кеңейтулерін уақытылы жаңартуды жүргізу, вирусқа қарсы БҚ қорғалған компьютерлерден сайттармен жұмыс істеу және сайт пен хостинг аккаунтына қол жеткізуге арналған парольдердің жария етілуіне жол бермеу.

Web-серверді қорғаудың жалпы әдістері

Серверге арналған үш қауіпсіздік деңгейін ерекшелендіруге болады:

1-деңгей. *Ең төменгі қауіпсіздік деңгейі.*

1. Қолданыстағы бағдарламалық қамтылымды жаңғырту және патчтер орнату.
2. Барлық серверлер үшін бірыңғай күйге келтірулер (саясаттар) қолдану.
3. Артық қосымшаларды жою.

2-деңгей. *Басып енуге қарсы іс-қимыл жасау.*

1. Сыртқы желіаралық экран орнату.
2. Қауіпсіздік жүйелерін қашықтықтан әкімшілендіру.
3. Скрипттерді пайдалануды шектеу.
4. Пакеттерді фильтрлеуді пайдалана отырып, Web-серверлерді қорғау.
5. Персоналды оқыту мен қол жеткізу құқықтарының аражігін ажырату.
6. 1-деңгейде аталған шешімдерді қолдану.

3-деңгей. *Шабылдарды айқындау және олардың ықпалын нашарлату.*

1. Басымдылықтарды бөлу.
2. Аппараттық қорғау жүйелері.
3. Ішкі желіаралық экран.
4. Басып енулерді айқындаудың желілік жүйелері.
5. Серверлерде (хосттарда) орнатылатын басып енулерді айқындау жүйелері.
6. 2-деңгейде аталған шешімдерді қолдану.

Web-серверлерді қорғаудың мына келесі ортақ әдістерін атауға болады:

- артық бағдарламалық қамтылымды (қосымшаларды) жою;
- Web-серверлердің қорғалуын бұзу әрекеттерін айқындау;
- орнатылған бағдарламалық қамтылымдағы ақауларды түзету;
- желіге жасалған шабуылдардың салдарын азайту;
- Web-сервер жария етілген жағдайда, желінің қалған бөлігін қорғау.