ДӘРІС №2: Желілік шабуылдар және оларды анықтау технологиялары

1) Желілік шабуылдардың негізгі түрлері;

2) Шабуылдарды анықтау технологиялары

1) Желілік шабуылдардың негізгі түрлері;

Барлық желілік шабуылдарды екі класқа бөлуге болады: пассивті және белсенді.

1.1. Пассивті шабуыл - бұл қарсыласы жіберілген хабарламаларды өзгерте алмайтын және өз хабарларын жіберуші мен алушының арасындағы ақпарат арнасына кіргізе алмайтын шабуыл. Пассивті шабуылдың мақсаты тек жіберілген хабарламаларды тыңдау және трафикті талдау болуы мүмкін. Бұл жағдайда құпиялылық бұзылады (1-сурет).

1-сурет. Пассивті шабуыл

Скан-шабуылдар - пассивті шабуылдардың бір түрі. Олар шабуылдаушы әр түрлі пакеттерді жіберу арқылы мақсатты желіні немесе жүйені тексерген кезде пайда болады. Бұл әдетте желілік осалдықтарды талдау құралдары арқылы жасалады, коммерциялық және ақысыз. Дәл осы құралдарды жүйелік әкімшілер өз жүйелеріндегі осалдықтарды табу үшін пайдаланады. Технологиялар бірдей, бірақ іс-әрекеттің уәжі басқаша!

Алынған жауаптарды талдау арқылы шабуылдаушы жүйенің сипаттамалары мен осалдықтары туралы көп біле алады. Сканерлеу шабуылы - шабуылдаушыға арналған нысанды анықтау құралы. Бұл шабуылдар жүйелерге енбейді немесе басқаша түрде ымыраға келмейді. Қолданылатын құралдардың әртүрлі атаулары бар: желілік анализаторлар, порт анализаторлары, желілік сканерлер, порт сканерлері немесе осалдық сканерлер.

Сканерлеу шабуылдары мыналарды анықтай алады:

- мақсатты желінің топологиясы;
- брандмауэр өткен желілік трафиктің түрлері;
- желідегі белсенді хосттар;
- хосттарда жұмыс істейтін операциялық жүйелер;

• хосттарда жұмыс жасайтын серверлік бағдарламалық жасақтама;

• барлық анықталған бағдарламалық жасақтама нұсқаларының нөмірлері.

Осалдық сканерлері - бұл хосттардың нақты осалдығын тексеретін сканерлердің ерекше түрі. Шабуылдаушы шабуылға осал болатын хосттар тізімін (IP-мекен-жайларды) анықтайтын осалдық сканерін іске қоса алады.

1.2 Белсенді шабуыл - бұл қарсыластың жіберілген хабарламаларды өзгертуге және өз хабарламаларын енгізуге мүмкіндігі болатын шабуыл. Белсенді шабуылдардың келесі түрлері бөлінеді:

Қызметтен бас тарту (DoS) шабуылы

Қызметтен бас тарту желілік қызметтердің қалыпты жұмысын бұзады. Мысалы, қарсылас белгілі бір алушыға бағытталған барлық хабарламаларды ұстай алады. Мұндай шабуылдың тағы бір мысалы - елеулі трафиктің жасалуы, соның салдарынан желілік қызмет заңды клиенттердің сұраныстарын өңдей алмайды. Бұл жағдайда олар қол жетімділіктің бұзылғанын айтады: шабуыл, егер ол заңды қолданушыға сол жерде жүйенің белгілі бір ресурсына, содан кейін оған қажет формада қол жеткізуге мүмкіндік бермесе, қол жетімділікті бұзады.

DoS шабуылдары мақсатты желідегі жүйелерді немесе қызметтерді баяулатуға немесе тоқтатуға тырысуы мүмкін. DoS шабуылдарының екі түрі бар: ауыр пайдалану және су тасқыны.

TCP / IP желілеріне мұндай шабуылдың классикалық мысалы - шабуылдаушы TCP байланысын орнатуды бастайтын пакеттерді жіберетін, бірақ осы байланысты орнатуды аяқтайтын пакеттерді жібермейтін SYN шабуылы. Нәтижесінде, сервер қосылу кестесінен асып кетуі мүмкін және сервер заңды қолданушылармен байланыс орната алмайды (2-сурет).

2- сурет. DoS шабуылы

Деректер ағынының модификациясы - «ортадағы адам» шабуылы (*man in the middle****)***

Деректер ағынының өзгеруі дегеніміз не жіберілетін хабарламаның мазмұнын өзгерту, не хабарламалар ретін өзгерту.

Бұл жағдайда олар тұтастықты бұзады дейді: шабуыл, егер ол шабуылдаушыға жүйенің күйін немесе жүйеде сақталған немесе берілетін деректерді өзгертуге мүмкіндік берсе, тұтастықты бұзады (3-сурет).

3-сурет. ***«Ортадағы адам» шабуылы (****man in the middle****)***

2) Шабуылдарды анықтау технологиялары

Қазіргі уақытта әртүрлі шабуылдардың түрлері бар:
- желіге әсер ету сипаты бойынша;
- әсер ету мақсаты бойынша;
- шабуылдалған желіден кері байланыстың болуы бойынша;
- шабуылдың басталу шарты бойынша;
- шабуыл нысанасының объектіге қатысты орналасуы бойынша;
- ISO сілтеме моделі деңгейінде.

Желілік және ақпараттық технологиялар тез өзгеретіні соншалық, статикалық басқару жүйелері, брандмауэрлер, аутентификация жүйелері, статикалық қорғаныс механизмдері көптеген жағдайларда тиімді қорғанысты қамтамасыз ете алмайды. Сондықтан да қауіпсіздіктің бұзылуын тез анықтау және алдын алу үшін динамикалық әдістер қажет. Дәстүрлі қол жетімділікті басқару модельдерін қолдану арқылы анықталмайтын бұзушылықтарды анықтай алатын технологиялардың бірі - бұл шабуылды анықтау технологиясы.

Негізінен, шабуылды анықтау процесі дегеніміз корпоративті желіде пайда болатын күдікті әрекетті бағалау процесі. Басқаша айтқанда, шабуылды анықтау - бұл есептеу немесе желілік ресурстарға бағытталған күдікті әрекеттерді анықтау және оларға жауап беру процесі.

Желілік ақпаратты талдау әдістері:
- статистикалық әдіс;
- эксперттік жүйелер;
- нейрондық желілер.