СӨЖ №2. Осалдықтарды анықтау және бағалау әдістері

Жұмыстың мақсаты

Ақпараттық жүйелердегі осалдықтарды анықтау, растау және тәуекелін бағалау әдістерін зерттеу, автоматтандырылған және сараптамалық тәсілдердің айырмашылығын салыстыру және семестрлік жоба үшін осалдықтарды бағалау тәртібін әзірлеу.

Пәнмен және жеке семестрлік жобамен байланысы

СӨЖ №2 ПЖ №9–10-дағы енуге тестілеу, ашық порттар, сервистер және attack surface талдауымен байланысты. Нәтижесі семестрлік жобаның vulnerability assessment және hardening бөліміне енгізіледі.

Қысқаша теориялық мәліметтер

Осалдық – жүйенің, бағдарламалық компоненттің, конфигурацияның немесе процестің қауіптің іске асуына мүмкіндік беруі мүмкін әлсіздігі. Осалдықты анықтау мен оны нақты тәуекел ретінде бағалау бірдей ұғым емес. Бір техникалық белгі әртүрлі активтерде әртүрлі салдарға әкелуі мүмкін.

Осалдықтарды анықтау активтерді түгендеуден және attack surface түсінуден басталады. Ашық порттар, сервистер, веб-интерфейстер, бағдарламалық нұсқалар және конфигурациялар зерттеледі. Бірақ ашық порт немесе ескі нұсқа туралы баннер автоматты түрде расталған осалдық болып саналмайды.

Автоматтандырылған vulnerability scanner белгілі шаблондар, нұсқалар және конфигурациялық белгілер бойынша ықтимал мәселелерді табуға көмектеседі. Оның артықшылығы – үлкен көлемдегі жүйелерді жүйелі тексеру. Шектеуі – false positive және контекстің жеткіліксіздігі. Сондықтан scanner finding міндетті түрде evidence және қолмен тексерумен толықтырылуы тиіс.

Сараптамалық бағалау осалдықтың нақты активке әсерін, exploitability шарттарын, қолданыстағы қорғаныс бақылауларын және бизнес контексті ескеруге мүмкіндік береді. Evidence мәселенің бар екенін қауіпсіз түрде көрсетуге жеткілікті болуы тиіс және зертханалық ортадан тыс рұқсатсыз әрекетке әкелмеуі керек.

CVSS техникалық ауырлықты стандартталған көрсеткіштер арқылы сипаттауға көмектеседі. Дегенмен CVSS нақты ұйымдағы актив құндылығын немесе барлық бизнес салдарын толық алмастырмайды. Сондықтан severity техникалық бағамен бірге exposure, актив маңыздылығы және қолданыстағы controls негізінде түсіндіріледі.

Осалдықтарды басымдықтау кезінде тек ең жоғары баллға сүйену жеткіліксіз. Интернеттен қолжетімділік, нақты сервис мақсаты, аутентификация, segmentation және remediation күрделілігі де ескеріледі. Бір осалдық сыртқы серверде жоғары, ал оқшауланған зертханалық сегментте төменірек операциялық тәуекел беруі мүмкін.

Бағалаудың соңғы кезеңі remediation және retest болып табылады. Түзету шарасы осалдықтың түпкі себебін азайтуы керек: жаңарту, конфигурацияны өзгерту, сервисті өшіру, қолжетімділікті шектеу немесе басқа hardening шарасы. Retest түзетудің шынымен орындалғанын және мәселенің жойылғанын тексереді.

Әдістемелік нұсқаулар

Зертханалық жүйе немесе оқытушы берген vulnerability findings үшін scope анықтаңыз. Активтер, сервистер және қолданылатын дереккөздерді сипаттап, автоматты сканер нәтижесін түпкілікті дәлел ретінде қабылдамаңыз.

Әр finding үшін evidence, ықтимал false positive, exposure және актив маңыздылығын талдаңыз. Расталған мәселелерді CVSS немесе басқа негізделген severity шкаласымен бағалап, техникалық баға мен нақты контексті бөлек көрсетіңіз.

Кемінде екі бағалау тәсілін салыстырыңыз: мысалы, scanner severity және контекстік тәуекел бағасы. Айырмашылықтардың себебін түсіндіріңіз және басымдықтау ережесін ұсыныңыз.

Әр маңызды осалдық үшін remediation шарасын және retest критерийін белгілеңіз. Нәтижені семестрлік жобаның vulnerability register артефактісі ретінде рәсімдеңіз.

Орындау тәртібі

1. Осалдық, finding, evidence, severity және risk ұғымдарының айырмашылығын көрсету.
2. Зертханалық жүйенің attack surface негізінде осалдықтарды анықтау көздерін жүйелеу.
3. Автоматты scanner нәтижелері мен сараптамалық тексеруді салыстыру.
4. Кемінде 5 finding үшін evidence және false positive ықтималдығын талдау.
5. Расталған мәселелердің severity/CVSS бағасын түсіндіру.
6. Exposure және актив маңыздылығын ескеріп басымдықтау.
7. Әр маңызды осалдық үшін remediation шарасын ұсыну.
8. Retest критерийлерін анықтап, vulnerability register дайындау.

Тапсырмалар

1. Осалдық, finding, evidence, severity және risk ұғымдарының айырмашылығын көрсету.
2. Зертханалық жүйенің attack surface негізінде осалдықтарды анықтау көздерін жүйелеу.
3. Автоматты scanner нәтижелері мен сараптамалық тексеруді салыстыру.
4. Кемінде 5 finding үшін evidence және false positive ықтималдығын талдау.
5. Расталған мәселелердің severity/CVSS бағасын түсіндіру.
6. Exposure және актив маңыздылығын ескеріп басымдықтау.
7. Әр маңызды осалдық үшін remediation шарасын ұсыну.
8. Retest критерийлерін анықтап, vulnerability register дайындау.

Орындау мысалы

Мысалы, scanner веб-сервер нұсқасына байланысты ықтимал осалдық көрсетеді. Магистрант сервис нұсқасын, конфигурациясын, exposure деңгейін және қолданыстағы қорғанысты тексеріп, finding-тің расталған немесе false positive екенін негіздейді. Содан кейін remediation және retest шарты жазылады.

Жеке тапсырма

Әр магистрант семестрлік жобасындағы бір актив немесе сервис тобын таңдап, кемінде бес ықтимал finding үшін жеке vulnerability register жасайды. Активтер немесе бағалау контексті қайталанбауы тиіс.

Нәтижелерді ұсыну формасы

– 5–7 бет есеп
– attack surface қысқаша сипаттамасы
– vulnerability register
– CVSS/контекстік бағалау кестесі
– remediation және retest жоспары
– семестрлік жобаға енгізілетін басымдықтау ережесі

Есепке қойылатын талаптар

Есепте жұмыстың мақсаты, зерттеу сұрағы, пайдаланылған деректердің немесе қауіпсіздік артефактілерінің шығу тегі, талдау әдісі, салыстыру критерийлері, нәтижелер

және олардың интерпретациясы берілуі тиіс. Қорытынды әрбір сандық немесе сапалық нәтижемен байланыстырылып, жұмыстың шектеулері көрсетіледі.

Код қолданылған жағдайда random_state немесе seed, split, preprocessing кезеңдері, негізгі параметрлер және бағдарламалық орта тіркеледі. Нәтижені тек кесте немесе метрика түрінде беру жеткіліксіз: магистрант алынған айырмашылықтардың себебін және нәтижені қандай жағдайда жалпылауға болмайтынын түсіндіреді.

Бағалау критерийлері

Критерий	**Үлес салмағы**
Теориялық негіз және терминдерді дұрыс қолдану	15%
Әдіс пен критерийлерді негіздеу	15%
Деректер/артефактілермен жұмыс	20%
Салыстыру және нәтижелерді талдау	20%
Жеке тапсырма және семестрлік жобамен байланыс	20%
Есепті рәсімдеу және дереккөздер	10%

Бақылау сұрақтары

1. Осалдық пен тәуекелдің айырмашылығы қандай?
2. Неліктен scanner finding түпкілікті дәлел емес?
3. Evidence қандай мақсатта қажет?
4. False Positive vulnerability assessment-ке қалай әсер етеді?
5. CVSS нені бағалайды?
6. Неліктен CVSS бизнес әсерді толық алмастырмайды?
7. Exposure нені білдіреді?
8. Осалдықтарды басымдықтау кезінде қандай факторлар ескеріледі?
9. Remediation мен mitigation айырмашылығы неде?
10. Retest не үшін жүргізіледі?

Әдебиеттер тізімі

1. Менщиков А.А., Заколдаев Д.А., Воробьева А.А. Введение в кибербезопасность и киберустойчивость: учебно-методическое пособие. Санкт-Петербург: Университет ИТМО, 2024. 72 с.

2. Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение: учебно-методическое пособие. Санкт-Петербург: Университет ИТМО, 2018. 45 с.

3. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. Екатеринбург: Издательство Уральского университета, 2019. 204 с.

4. Шаньгин В.Ф. Информационная безопасность: учебное пособие. Москва: ДМК Пресс, 2014. 702 с.

5. Назарян А.К., Карцан И.Н. Современные кибератаки: классификация и способы защиты // Информатика. Экономика. Управление. 2025. Т. 4, № 1. С. 1001–1007.

6. Лукьянец С.Е. Гибридные системы кибербезопасности: искусственный интеллект и анализ сетевого трафика для противодействия современным угрозам.

7. Сигалов Д.А. Методы выявления поверхности атаки веб-приложений при помощи анализа клиентского JavaScript-кода: диссертация. Москва: МГУ имени М.В. Ломоносова, 2024.

8. Кривчун Н.А., Солодовников Д.В., Соколов А.К., Шорохов К.Д., Кучук М.И. Кибератаки и методы их предотвращения в информационных системах // Дискуссия. 2024. Вып. 128. С. 120–126.