Многопрофильная инженерная олимпиада «Звезда»
«Информационная безопасность»

7-9 классы **Заключительный этап** **2020-2021**

Задания, ответы и критерии оценивания

Задача 1. Посчитать значение вектора уязвимости CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N согласно стандарту CVSS версии 3.1. *(12 баллов)*

Решение. ISS = 1 – [(1 – Confidentiality) x (1 – Integrity) x (1 – Availability)] = 1 – [(1 – 0.22) x (1– 0) x (1 – 0)] = 0.22
Impact = 6.42 x ISS = 6.42 x 0.22 = 1.4124
Exploitability = 8.22 x AttackVector x AttackComplexity x PrivilegesRequired x UserInteraction = 8.22 x 0.85 x 0.77 x 0.85 x 0.85 = 3.887042775
BaseScore = Roundup (Minimum [(Impact + Exploitability), 10]) = Roundup (Minimum [(1.4124 + 3.887042775), 10]) = Roundup (Minimum [5.299442775, 10]) = 5.3

№ критерия	Количество баллов	Описание критерия
1	12	Приведено правильное решение, получен верный ответ. Допускается отклонение от ответа на 0.2
2	8	Приведено правильное решение, получен неверный ответ
3	2	Решение недостаточное или не приведено, ответ верный

Задача 2. Опишите значения метрик вектора уязвимости CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N. *(9 баллов)*

Решение. AV:N – уязвимость, доступная для удаленного использования;
AC:L – никаких специальных условий или передовых знаний для совершения атаки не требуется;
PR:N – для совершения атаки не требуется авторизация и привилегии;
UI:R – для успешного использования этой уязвимости от пользователя требуется предпринять некоторые действия (например, переход по ссылке, установка приложения, открытие файла и т.д.);
S:U – эксплуатация уязвимости не позволяет нарушить конфиденциальность, целостность и доступность какого-либо другого компонента системы, кроме уязвимого;
C:H – полная потеря конфиденциальности, в результате чего все ресурсы в затронутом компоненте раскрываются злоумышленнику;
I:L – модификация данных возможна, но злоумышленник не может контролировать последствия модификации, либо количество изменений ограничено. Изменение данных не оказывает прямого серьезного влияния на затронутый компонент;
A:N – нет никакого влияния на доступность затронутого компонента.

№ критерия	Количество баллов	Описание критерия
1	9	Все метрики описаны верно. Возможен вариант ответа с описанием атаки без описания каждой конкретной метрики
2	5	В 1 – 2 метриках допущены ошибки, либо описание отсутствует
3	1	Решение частично верное, но недостаточное. Либо ошибки допущены более, чем в двух метриках.

Задача 3. Посчитать оценку окружения уязвимости с учетом следующих значений метрик окружения CVSS:3.1/MAV:A/MAC:H/MPR:L/MUI:N/MS:C/MC:H/MI:H/MA:L/A:H/E:F/RL:O/RC:C. *(13 баллов)*

Решение. MISS = Minimum (1 – [(1 – ConfidentialityRequirement x ModifiedConfidentiality) x (1 – IntegrityRequirement x ModifiedIntegrity) x (1 – AvailabilityRequirement x ModifiedAvailability)], 0.915) = Minimum (1 – [(1 – 1 x 0.56) x (1 – 1 x 0.56) x (1 – 1 x 0.22)], 0.915) = 0.848992
ModifiedImpact = 7.52 x (MISS – 0.029) – 3.25 x (MISS x 0.9731 – 0.02)^{13} = 7.52 x (0.848992– 0.029) – 3.25 x (0.848992x 0.9731 – 0.02) ^{13} ≈ 6.16633984 – 0.19738691 = 5.96895293
ModifiedExploitability = 8.22 x ModifiedAttackVector x ModifiedAttackComplexity x ModifiedPrivilegesRequired x ModifiedUserInteraction = 8.22 x 0.62 x 0.44 x 0.68 x 0.85 = 1.296116448
EnvironmentalScope = Roundup (Roundup [Minimum (1.08 x [ModifiedImpact + ModifiedExploitability], 10)] x ExploitCodeMaturity x RemediationLevel x ReportConfidence) = Roundup (Roundup [Minimum (1.08 x [5.96895293 + 1.296116448], 10)] x 0.97 x 0.95 x 1) = Roundup (7.9 x 0.97 x 0.95 x 1) = 7.3

№ критерия	Количество баллов	Описание критерия
1	13	Приведено правильное решение, получен верный ответ. Допускается отклонение от ответа на 0.2
2	8	Приведено правильное решение, получен неверный ответ
3	2	Решение недостаточное или не приведено, ответ верный

Задача 4. По описанию атаки составить базовый вектор уязвимости CVSS версии 3.1 и посчитать его значение. Microsoft Internet Explorer с 9 по 11 версию некорректно обрабатывает объекты в памяти, что позволяет атакующему выполнить произвольный код на системе при переходе пользователя по ссылке, содержащей вредоносный код. Злоумышленник может выполнить данную атаку удаленно. *(15 баллов)*

Решение. CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
ISS = 1 – [(1 – Confidentiality) x (1 – Integrity) x (1 – Availability)] = 1 – [(1 – 0.56) x (1– 0.56) x (1 – 0.56)] = 0.914816
Impact = 6.42 x ISS = 6.42 x 0.914816= 5.87311872
Exploitability = 8.22 x AttackVector x AttackComplexity x PrivilegesRequired x UserInteraction = 8.22 x 0.85 x 0.77 x 0.85 x 0.62 = 2.83525473
BaseScore = Roundup (Minimum [(Impact + Exploitability), 10]) = Roundup (Minimum [(5.87311872 + 2.83525473), 10]) = Roundup (Minimum [8.70837345, 10]) = 8.8

№ критерия	Количество баллов	Описание критерия
1	15	Учеником составлен правильный вектор, приведено правильное решение, получен верный ответ. Допускается отклонение от ответа на 0.2
2	10	Составлен правильный вектор, приведено правильное решение, получен неверный ответ.
3	8	Вектор составлен с ошибкой в 1 метрике, приведено правильное решение, получен верный ответ (для составленного учеником вектора).
4	4	Вектор составлен с ошибкой более чем в 1 метрике, приведено правильное решение, получен верный ответ (для составленного учеником вектора).
5	2	Решение недостаточное или не приведено, ответ верный

Задача 5. Определить какая из уязвимостей критичнее. Проверить правильность с помощью расчета значения вектора CVSS.

А) Алгоритм аутентификации в кардиостимуляторах Abbott Laboratories, изготовленных до 28 августа 2017 г., который включает ключ аутентификации и отметку времени, может быть

скомпрометирован или обойден, что может позволить злоумышленнику, находящемуся поблизости, передать несанкционированные команды кардиостимулятору через радиочастотную связь.

Б) Эта уязвимость позволяет удаленным злоумышленникам выполнить произвольный код на уязвимых установках Google Chrome. Для использования этой уязвимости требуется взаимодействие с пользователем, поскольку жертва должна посетить вредоносную страницу или открыть вредоносный файл. Конкретный недостаток существует в обработке изображений JPEG 2000. Специально созданное изображение JPEG 2000, встроенное в PDF-файл, может заставить Google Chrome записывать в память за пределами выделенного объекта. Злоумышленник может использовать эту уязвимость для выполнения произвольного кода в контексте текущего процесса.
Злоумышленник создает PDF-файл, содержащий вредоносное изображение JPEG 2000. Это делается доступным для жертв, например, через веб-страницу. Жертва открывает PDF-документ в браузере Google Chrome, и браузер отображает PDF-файл с помощью встроенного средства просмотра PDFium PDF. Это включает эксплойт и запускает исполняемый код, который злоумышленник поместил в образ, захватывая браузер. *(20 баллов)*

Решение. А) CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
ISS = 1 – [(1 – Confidentiality) x (1 – Integrity) x (1 – Availability)] = 1 – [(1 – 0.56) x (1– 0.56) x (1 – 0.56)] = 0.914816
Impact = 6.42 x ISS = 6.42 x 0.914816= 5.87311872
Exploitability = 8.22 x AttackVector x AttackComplexity x PrivilegesRequired x UserInteraction = 8.22 x 0.62 x 0.44 x 0.85 x 0.85 = 1.62014556
BaseScore = Roundup (Minimum [(Impact + Exploitability), 10]) = Roundup (Minimum [(5.87311872 + 1.62014556), 10]) = Roundup (Minimum [7.49326428, 10]) = 7.5

Б) CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
ISS = 1 – [(1 – Confidentiality) x (1 – Integrity) x (1 – Availability)] = 1 – [(1 – 0.56) x (1– 0.56) x (1 – 0.56)] = 0.914816
Impact = 6.42 x ISS = 6.42 x 0.914816= 5.87311872
Exploitability = 8.22 x AttackVector x AttackComplexity x PrivilegesRequired x UserInteraction = 8.22 x 0.85 x 0.77 x 0.85 x 0.62 = 2.83525473
BaseScore = Roundup (Minimum [(Impact + Exploitability), 10]) = Roundup (Minimum [(5.87311872 + 3.887042775), 10]) = Roundup (Minimum [8.70837345, 10]) = 8.8

№ критерия	Количество баллов	Описание критерия
1	20	Учеником представлено его видение приоритетной уязвимости. Составлены правильные вектора, приведено правильное решение, получены верные ответы при расчетах. Допускается отклонение от ответа на 0.2
2	17	Учеником не описаны основания для определения какой-либо из уязвимостей наиболее приоритетной. Составлены правильные вектора, приведено правильное решение, получены верные ответы при расчетах. Допускается отклонение от ответа на 0.2
3	15	Учеником представлено его видение приоритетной уязвимости. Составлены правильные вектора, приведено правильное решение, получен неверный ответ.
4	12	Учеником не описаны основания для определения какой-либо из уязвимостей наиболее приоритетной. Составлены правильные вектора, приведено правильное решение, получен неверный ответ.
5	10	Учеником представлено его видение приоритетной уязвимости. При составлении векторов допущена ошибка в 1 метрике (возможно по 1 в каждом), приведено правильное решение, получен верный ответ (для составленного учеником вектора).
6	7	Учеником не описаны основания для определения какой-либо из уязвимостей наиболее приоритетной. При составлении векторов допущена ошибка в 1 метрике (возможно по 1 в каждом), приведено правильное решение, получен верный ответ (для составленного учеником вектора).

7	5	Учеником представлено его видение приоритетной уязвимости. Вектор составлен с ошибкой более чем в 1 метрике, приведено правильное решение, получен верный ответ (для составленного учеником вектора).
8	3	Учеником не описаны основания для определения какой-либо из уязвимостей наиболее приоритетной. Вектор составлен с ошибкой более чем в 1 метрике, приведено правильное решение, получен верный ответ (для составленного учеником вектора).
9	2	Учеником представлено его видение приоритетной уязвимости. Решение недостаточное или не приведено, ответ верный

Проектная задача. Итоговый показатель критичности не всегда определяется метриками CVSS. Также данный метод плохо подходит для производственных объектов, так как не учитывает физические составляющие системы. Предложите свою идею оценки рисков и методику ее расчета. Для корректной оценки задания необходимо привести примеры расчета. *(31 балл)*

№ критерия	Количество баллов	Описание критерия
1	31	Учеником описаны критерии оценки риска (5 и более), обоснована методика оценки, приведены расчетные формулы. Примеры демонстрируют логичность приведенной методики.
2	21	Учеником описаны критерии оценки риска (менее 5), обоснована методика оценки, приведены расчетные формулы. Примеры демонстрируют логичность приведенной методики.
3	15	Учеником описаны критерии оценки риска, обоснована методика оценки, приведены расчетные формулы. Примеры не позволяют оценить логичность приведенной методики.
4	10	Учеником описаны критерии оценки риска, обоснована методика оценки, приведены расчетные формулы. Примеры не приведены.
5	3	Описаны критерии оценки риска, имеются наброски методики и формул.