Cybersecurity Quiz Pack White2hack

theory, practice, web, Windows, Linux, cloud, hack culture and history

Квиз White2Hack

Legend: желтая подсветка = правильный ответ

Q01 • Security basics • Level: Easy

1. Что означает классическая CIA triad в cybersecurity?

A. Confidentiality, Integrity, Availability
B. Compliance, Inspection, Authorization
C. Cloud, Identity, Automation
D. Containment, Investigation, Attribution

Q02 • Security basics • Level: Easy

2. Какой принцип лучше всего описывает фразу: "дать пользователю ровно столько прав, сколько нужно для работы, и не больше"?

A. Security through obscurity
B. Least privilege
C. Defense in depth
D. Fail open

Q03 • Identity • Level: Medium

3. Какой вариант MFA обычно считают более устойчивым к phishing, чем одноразовые SMS-коды?

A. SMS OTP на телефон
B. Пароль + секретный вопрос
C. FIDO2/WebAuthn passkey или аппаратный security key
D. PIN-код, записанный в password hint

Q04 • Governance • Level: Medium

4. В NIST CSF 2.0 появилась отдельная верхнеуровневая функция. Какая?

A. Hunt
B. Govern
C. Exploit
D. Patch

Q05 • Threat modeling • Level: Medium

5. Что такое threat model в нормальном engineering sense?

A. Список CVE за последний месяц
B. Документ, который помогает понять assets, trust boundaries, threats и mitigations
C. Автоматический отчет антивируса
D. Только список firewall rules

Q06 • Web/AppSec • Level: Easy

6. Какая редакция OWASP Top 10 является актуальной выпущенной версией для web application security на момент подготовки этого сборника?

A. OWASP Top 10:2017
B. OWASP Top 10:2021
C. OWASP Top 10:2025
D. OWASP Top 10:2030 draft

Q07 • Web/AppSec • Level: Medium

7. Пользователь меняет в URL /api/orders/1001 на /api/orders/1002 и видит чужой заказ. Какой это класс проблем?

A. Broken Access Control / IDOR
B. DNS cache poisoning
C. Clickjacking only
D. Path MTU discovery issue

Q08 • Web/AppSec • Level: Easy

8. Что является самым надежным baseline-защитным приемом против SQL injection в приложении?

A. Черный список слов SELECT и UNION
B. Prepared statements / parameterized queries
C. Спрятать ошибку базы данных красивой 500-страницей
D. Переименовать таблицы в непонятные имена

Q09 • Web/AppSec • Level: Medium

9. Stored XSS отличается от reflected XSS тем, что...

A. stored XSS хранится на сервере или в хранилище приложения и потом отдается другим пользователям
B. stored XSS работает только в старом Internet Explorer
C. reflected XSS никогда не использует JavaScript
D. stored XSS невозможен в SPA

Q10 • Web/AppSec • Level: Medium

10. Какая связка обычно помогает против CSRF в web-приложениях?

A. Только смена User-Agent
B. CSRF token + SameSite cookies + проверка unsafe methods
C. Отключить HTTPS
D. Сделать все endpoints GET-only

Q11 • Cloud/Web • Level: Hard

11. SSRF становится особенно неприятным в cloud, когда приложение может достучаться до...

A. только favicon.ico

B. metadata service или internal-only endpoints

C. публичной страницы документации

D. статичного CSS-файла

Q12 • API Security • Level: Medium

12. В OWASP API Security Top 10 2023 риск API1 называется...

A. Broken Object Level Authorization

B. Weak TLS Cipher Suites

C. Open Redirect

D. Malicious CSS Injection

Q13 • API Security • Level: Medium

13. API endpoint /export принимает огромный date range и кладет сервер на CPU/DB. Это ближе всего к какому API risk?

A. Unrestricted Resource Consumption

B. Clickjacking

C. DNSSEC downgrade

D. Binary planting

Q14 • DevSecOps • Level: Easy

14. SCA tool в DevSecOps обычно нужен, чтобы...

A. рисовать ER-диаграммы базы

B. искать уязвимые open-source dependencies и license risks

C. заменять code review

D. шифровать весь трафик в браузере

Q15 • Supply chain • Level: Medium

15. SBOM - это, простыми словами...

A. список компонентов, библиотек и версий, из которых собран софт

B. обязательный firewall rulebook

C. таблица паролей сервисных аккаунтов

D. режим запуска контейнера от root

Q16 • Secrets • Level: Easy

16. Что лучше всего делать с API key, случайно попавшим в публичный GitHub repo?

A. Просто удалить строку из последнего коммита

B. Срочно revoke/rotate ключ и очистить историю, если нужно

C. Переименовать переменную

D. Добавить комментарий "do not use"

Q17 • Crypto • Level: Medium

17. Как правильно хранить пользовательские пароли в базе?

A. В plaintext, но база за firewall
B. MD5(password) без salt
C. Argon2id/bcrypt/scrypt с уникальной salt и адекватными cost parameters
D. AES-encrypt одним ключом, лежащим рядом в config.json

Q18 • AppSec mindset • Level: Medium

18. Почему фраза "у нас есть WAF, значит AppSec больше не нужен" - красный флаг?

A. WAF всегда ломает HTTPS
B. WAF - compensating control, но не заменяет secure design, code review и fixing root cause
C. WAF защищает только от фишинга
D. WAF не умеет работать с HTTP

Q19 • Windows logging • Level: Medium

19. Windows Security Event ID 4625 обычно связан с...

A. успешным запуском службы
B. failed logon attempt
C. очисткой корзины
D. изменением часового пояса

Q20 • Windows monitoring • Level: Medium

20. Sysmon в enterprise/security context обычно используют для...

A. детального логирования процессов, сетевых соединений и других событий endpoint telemetry
B. дефрагментации SSD
C. замены Active Directory
D. визуального редактирования реестра

Q21 • Windows/PowerShell • Level: Hard

21. Почему PowerShell Execution Policy не стоит считать полноценной security boundary?

A. Потому что это convenience/safety feature, которую можно обходить разными легитимными путями
B. Потому что PowerShell не умеет запускать скрипты
C. Потому что она шифрует все файлы
D. Потому что работает только в Linux

Q22 • Windows permissions • Level: Medium

22. Почему share/NTFS permission "Everyone: Full Control" на рабочей папке - smell?

A. Это всегда ускоряет бэкапы
B. Это может привести к несанкционированному чтению, изменению или удалению данных
C. Это автоматически включает MFA
D. Это запрещает доступ администраторам

Q23 • Active Directory • Level: Easy

23. Членство в какой группе обычно дает крайне высокие привилегии в домене AD?

A. Domain Admins

B. Remote Desktop Users на одной workstation

C. Domain Guests

D. Printer Operators в тестовом OU

Q24 • Active Directory • Level: Hard

24. Kerberoasting чаще всего связан с какими учетками?

A. service accounts с SPN и слабым/долго не меняемым паролем

B. локальными гостевыми пользователями без сети

C. только учетками macOS

D. только учетками без Kerberos

Q25 • Active Directory • Level: Medium

25. Для чего обычно используют Windows LAPS / подходы managed local admin passwords?

A. Чтобы у всех машин был один общий локальный admin password

B. Чтобы управлять уникальными локальными admin passwords и регулярно их ротировать

C. Чтобы отключить audit logs

D. Чтобы заменить DNS

Q26 • Linux • Level: Easy

26. Команда sudo -l в Linux обычно показывает...

A. какие команды текущий пользователь может запускать через sudo

B. список всех открытых портов

C. пароли всех пользователей

D. температуру CPU

Q27 • Linux/SSH • Level: Medium

27. Какие права обычно ставят на приватный SSH key пользователя?

A. 777

B. 600

C. 000 навсегда

D. 755

Q28 • Linux/SSH • Level: Medium

28. Какой hardening-подход для SSH чаще всего считается хорошей практикой?

A. разрешить root login по паролю из интернета

B. использовать keys/MFA, отключить password login где возможно и запретить root login

C. поставить пароль qwerty, но длинный баннер

D. открыть SSH на всех интерфейсах без логирования

Q29 • Linux audit • Level: Hard

29. Что ищет команда вида find / -perm -4000 -type f 2>/dev/null?

A. файлы с SUID bit

B. только пустые папки

C. все файлы больше 4 GB

D. только broken symlinks

Q30 • Linux networking • Level: Medium

30. Команда ss -tulpen чаще всего используется, чтобы посмотреть...

A. listening TCP/UDP sockets, процессы и порты

B. пароли в браузере

C. разметку диска в GUI

D. историю git-коммитов

Q31 • DNS • Level: Hard

31. DNS zone transfer (AXFR), если он случайно разрешен всем, опасен потому что...

A. может раскрыть внутреннюю карту DNS-имен и инфраструктурные подсказки

B. автоматически шифрует домен

C. делает сайт быстрее

D. удаляет все MX-записи

Q32 • Database security • Level: Medium

32. Для production-приложения плохая идея подключаться к базе под учеткой с правами DBA, потому что...

A. это увеличивает blast radius при компрометации приложения

B. это всегда снижает latency

C. это отключает SQL injection автоматически

D. DBA-учетка не умеет читать таблицы

Q33 • Ransomware defense • Level: Medium

33. Какой контроль особенно важен против ransomware-impact, а не только initial access?

A. immutable/offline backups с регулярным restore testing

B. красивый баннер на login screen

C. запретить всем пользователям менять wallpaper

D. поставить сложный hostname

Q34 • Detection • Level: Easy

34. SIEM в security operations нужен в первую очередь для...

A. централизации логов, корреляции событий, alerting и расследований

B. ускорения компиляции кода

C. замены всех EDR

D. создания HTML-страниц

Q35 • MITRE ATT&CK • Level: Medium

35. В MITRE ATT&CK тактика (tactic) - это...

A. цель или "why" действия атакующего, например Persistence или Defense Evasion

B. конкретная строка кода exploit

C. версия операционной системы

D. обязательный CVSS score

Q36 • Detection/IR • Level: Medium

36. Living off the land в атаке означает, что злоумышленник...

A. использует встроенные легитимные tools системы, чтобы меньше палиться

B. обязательно приносит свой kernel driver

C. атакует только IoT-устройства

D. работает без каких-либо команд

Q37 • Vulnerability management • Level: Medium

37. Зачем security-командам смотреть CISA KEV Catalog, а не только сортировать все по CVSS?

A. KEV показывает уязвимости с подтвержденной эксплуатацией в дикой природе

B. KEV содержит только теоретические баги без эксплуатации

C. CVSS всегда показывает бизнес-ущерб идеально

D. KEV нужен только для дизайна логотипов

Q38 • Cyber history • Level: Medium

38. Morris Worm 1988 известен тем, что...

A. стал одним из первых крупных инцидентов в интернете и повлиял на развитие incident response

B. был первым мобильным ransomware для Android

C. атаковал только Windows 11

D. создал технологию blockchain

Q39 • Malware history • Level: Medium

39. CIH / Chernobyl virus был особенно знаменит тем, что...

A. мог повреждать данные на диске и Flash BIOS на некоторых Windows 9x системах

B. был первым легальным antivirus plugin

C. работал только на iPhone

D. шифровал облачные buckets через OAuth

Q40 • Cyber history • Level: Easy

40. Кевин Митник чаще всего ассоциируется не только с hacking, но и с...

A. social engineering

B. созданием стандарта Wi-Fi 7

C. разработкой ядра Linux

D. изобретением SQL

Q41 • Cyber history • Level: Medium

41. История Владимира Левина обычно связывается с...

A. делом о несанкционированных переводах из Citibank в 1990-х

B. созданием протокола TLS 1.3

C. первым exploit для Kubernetes

D. авторством OWASP Top 10

Q42 • Threat modeling • Level: Medium

42. Что входит в STRIDE threat modeling mnemonic?

A. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

B. Scan, Trace, Run, Inject, Dump, Escape

C. SSL, TLS, RSA, IDS, DNS, EDR

D. Search, Tag, Report, Index, Delete, Export

Q43 • Cloud security • Level: Easy

43. Shared responsibility model в cloud означает, что...

A. провайдер отвечает вообще за все, клиент ни за что

B. ответственность делится между cloud provider и customer в зависимости от сервиса

C. клиент отвечает за физическую охрану дата-центра AWS/Azure/GCP

D. модель применяется только к домашним роутерам

Q44 • Cloud security • Level: Medium

44. Публичный S3 bucket / object storage с sensitive data - это прежде всего...

A. data exposure из-за misconfiguration

B. улучшение availability без рисков

C. нормальный способ секретного обмена паролями

D. пример сильной криптографии

Q45 • Kubernetes/Cloud • Level: Medium

45. Команда kubectl auth can-i полезна для...

A. проверки, разрешено ли субъекту выполнять конкретное действие в Kubernetes RBAC

B. шифрования etcd одним кликом

C. удаления всех pods без подтверждения

D. сканирования Docker Hub на malware

Q46 • Container security • Level: Medium

46. Какой container hardening-подход обычно правильнее?

A. запускать контейнеры от root и давать privileged: true всем

B. минимальный base image, non-root user, drop capabilities, read-only filesystem где возможно

C. класть SSH private key в image layer

D. обновления не нужны, если image маленький

Q47 • Email/Phishing • Level: Easy

47. Какая комбинация email security controls помогает снизить spoofing и phishing?

A. SPF, DKIM, DMARC + user awareness + reporting workflow

B. только красивый HTML-шаблон письма

C. отключение всех MX-записей

D. пароль admin/admin на почтовом сервере

Q48 • Incident response • Level: Medium

48. Что в IR обычно означает containment?

A. ограничение распространения инцидента и уменьшение ущерба до полного remediation

B. публикация поста в LinkedIn до анализа

C. удаление всех логов для экономии места

D. немедленная переустановка всех систем без triage

Q49 • Web/AppSec • Level: Medium

49. Какой HTTP response header помогает браузеру включать более строгую защиту от clickjacking?

A. X-Frame-Options или CSP frame-ancestors

B. Content-Length

C. Server-Timing только

D. Accept-Language

Q50 • Privacy/Data • Level: Easy

50. Data minimization в security/privacy context означает...

A. собирать и хранить только те данные, которые реально нужны

B. собирать все данные "на всякий случай"

C. хранить пароли в логах для удобства support

D. никогда не удалять старые дампы

Почему: *Чем меньше sensitive data хранится без необходимости, тем меньше legal, privacy и breach impact.*

Q51 • Windows/AD audit • Level: Medium

51. Нужно быстро найти отключенные учетные записи пользователей в Active Directory. Какая PowerShell-команда выглядит как нормальный defensive audit, а не random magic?

A. Get-ADUser -Filter * | Where-Object {$_.Enabled -eq $true}

B. Search-ADAccount -AccountDisabled -UsersOnly

C. Get-LocalUser | Where-Object Enabled -eq $false

D. net user /domain /disabled

E. Get-ADComputer -AccountDisabled -UsersOnly

Q52 • Linux audit • Level: Medium

52. Какой вариант команды чаще используют, чтобы найти SUID-файлы на текущем файловом разделе без ухода в другие mount points?

A. find / -xdev -type f -perm -4000 -ls

B. grep -R "suid" /etc/passwd

C. chmod -R u+s / 2>/dev/null

Q53 • PowerShell/Blue Team • Level: Easy

53. Что покажет команда Get-Process | Sort-Object CPU -Descending | Select-Object -First 5?

A. Пять процессов с наименьшим PID

B. Пять процессов, отсортированных по имени пользователя

C. Пять процессов с наибольшим накопленным CPU time

D. Пять последних событий в Windows Security log

Q54 • Windows Event Logs • Level: Medium

54. Что в большинстве Windows-аудитов ищет такая команда: Get-WinEvent -FilterHashtable @{LogName="Security"; Id=4625} -MaxEvents 20?

A. Последние 20 failed logon events

B. Последние 20 успешных установок драйверов

C. Все события PowerShell Script Block Logging

D. Список локальных администраторов

E. Только Kerberos Golden Ticket events

Q55 • Hacker culture • Level: Easy

55. С чем чаще всего связывают легенду Kevin Mitnick в массовой культуре security, если отбросить голливудский шум?

A. С изобретением SQL injection

B. С social engineering, phone phreaking и последующей карьерой security consultant

C. С созданием Stuxnet

D. С первым публичным exploit для Log4Shell

E. С авторством OWASP Top 10

Q56 • Cybercrime history • Level: Medium

56. Почему имя Vladimir Levin часто всплывает в разговорах про ранний cybercrime и banking security?

A. Его связывают с попыткой перевода миллионов долларов из Citibank в 1994 году

B. Он написал Morris Worm

C. Он первым описал STRIDE threat modeling

D. Он основал проект Metasploit

Q57 • ICS/OT history • Level: Medium

57. Что делало Stuxnet особенно знаковым кейсом для мира ICS/OT security?

A. Это был обычный phishing kit для кражи паролей от Gmail

B. Он был нацелен на PLC/промышленное оборудование и связывается с саботажем иранских центрифуг

C. Он шифровал домашние компьютеры и требовал выкуп в Bitcoin

D. Он появился как учебный worm в университетской лаборатории и не выходил за ее пределы

E. Он был первым браузерным adware для Windows 95

Q58 • APT/Threat intel • Level: Medium

58. APT28 / Fancy Bear в threat intel чаще всего атрибутируют какой стороне?

A. Финансово мотивированной группе из Бразилии

B. Российской военной разведке/GRU-linked activity cluster

C. Случайному botnet без политического контекста

D. Academic research team из Европы

Q59 • APT/Financial ops • Level: Medium

59. Какой ответ лучше всего описывает Lazarus Group в современной threat intel картине?

A. North Korea-linked state-sponsored group, связанная с espionage, destructive attacks и financial cyber operations

B. Открытое сообщество bug bounty hunters из Сан-Франциско

C. Название антивирусного движка для Linux servers

D. Группа, известная только defacement-атаками без malware и без финансовой мотивации

Q60 • Ethical hacking culture • Level: Easy

60. Что в индустрии обычно означает responsible disclosure / coordinated vulnerability disclosure?

A. Тихо продавать 0-day на underground-форумах

B. Сначала публично публиковать exploit, а потом писать vendor-у

C. Сообщить о баге владельцу системы, дать разумное время на fix и уже потом раскрывать детали согласованно

Карта ответов

Здесь представлен номер вопроса и буква правильного ответа. Таблица готова для загрузки в бота. Полный текст правильного варианта уже подсвечен желтым прямо в карточке вопроса.

#	Ответ	#	Ответ	#	Ответ	#	Ответ
1	A	2	B	3	C	4	B
5	B	6	C	7	A	8	B
9	A	10	B	11	B	12	A
13	A	14	B	15	A	16	B
17	C	18	B	19	B	20	A
21	A	22	B	23	A	24	A
25	B	26	A	27	B	28	B
29	A	30	A	31	A	32	A
33	A	34	A	35	A	36	A
37	A	38	A	39	A	40	A
41	A	42	A	43	B	44	A
45	A	46	B	47	A	48	A
49	A	50	A	51	B	52	A
53	C	54	A	55	B	56	A
57	B	58	B	59	A	60	C