**“Ethical hacking II” fanidan yakuniy nazorat savollar**

1. “Gray hat hacking”ning “white hat” va “black hat” xakerlikdan farqlarini tushuntiring.
2. “Gray hat” xakerlarning faoliyati qonuniyligini baholang, fikrlaringizni misollar bilan izohlang.
3. “White hat hacking” va “gray hat hacking” faoliyatini solishtiring.
4. Qanday holatlarda “gray hat” xakerlik foydali bo‘lishi mumkin?
5. “Gray hat” xakerlik axloqiy jihatdan qachon qabul qilinishi mumkin?
6. Jamiyat xavfsizligini ta’minlashda “gray hat hacking” qanday rol o‘ynaydi?
7. Qanday holatlarda “gray hat hacking” noqonuniy deb hisoblanadi?
8. “Gray hat” xakerlarning yirik kompaniyalar bilan ishlashi qanday qonuniy masalalarni keltirib chiqaradi?
9. Kiberxavfsizlikda “gray hat hacking” ning ijobiy va salbiy tomonlarini tahlil qiling.
10. Xakerlikning etika me’yorlari haqida yozing.
11. “Reverse engineering” tushunchasini izohlang.
12. Dasturiy ta’minotni tahlil qilishda “reverse engineering” qanday ishlatiladi?
13. “Ghidra” vositasining asosiy imkoniyatlarini tushuntiring.
14. “IDA Pro” va “Ghidra” o‘rtasidagi asosiy farqlarni izohlang.
15. “Reverse engineering”ni qonuniy jihatdan tahlil qiling.
16. “Reverse engineering” vositalari kiberxavfsizlikda qanday muhim rol o‘ynaydi?
17. “Ghidra” yordamida oddiy eksploitni tahlil qilish jarayonini yozib bering.
18. “IDA Pro” yordamida dasturiy eksploitni aniqlash usulini tushuntiring.
19. “Reverse engineering”da kodning shifrlangan qismini qanday aniqlash mumkin?
20. “Reverse engineering” va eksploit tahlil qilishni bir-biriga bog‘lab tushuntiring.
21. Exploit yaratish jarayonida dasturchi qanday xavflarga duch keladi?
22. Linux eksploitlarining Windows eksploitlaridan asosiy farqlari nima?
23. Exploitni samaradorligini oshirish uchun qanday usullar qo‘llaniladi?
24. Linux tizimida ishlatiladigan asosiy xavfsizlik cheklovlarini tushuntiring.
25. “Windows kernel” eksploitlari qanday xavflarni keltirib chiqaradi?
26. Kernel eksploitlarining tahlilini tushuntiring.
27. “PowerShell” eksploitlari boshqa eksploitlardan nimasi bilan farq qiladi?
28. Kernel darajasidagi eksploitlarni cheklovchi texnologiyalarni izohlang.
29. Exploitlardan himoyalanishning samarali usullari haqida yozing.
30. “ASLR (Address Space Layout Randomization)” qanday ishlaydi?
31. “Red Team” va “Blue Team” o‘rtasidagi asosiy farqlarni izohlang.
32. “Purple Team” qanday vazifalarni bajaradi?
33. “Red Team” hujumlari qanday qilib “Purple Team” tomonidan nazorat qilinadi?
34. “Purple Team” faoliyatini tashkil qilishda duch kelinadigan muammolarni izohlang.
35. “Red Team” va “Purple Team” ning birgalikdagi ishlash afzalliklari qanday?
36. Kiberxavfsizlik strategiyasida “Red Team” ning roli.
37. “Purple Team” ning tashkilot xavfsizligini yaxshilashdagi roli.
38. “Red Team” hujumining asosiy bosqichlarini tushuntiring.
39. “Blue Team” qanday himoya strategiyalarini qo‘llaydi?
40. “Purple Team” faoliyatida qanday vositalar muhim rol o‘ynaydi?
41. “Command and Control” tizimlari qanday ishlaydi?
42. C2 tizimlari qanday tahdidlarni keltirib chiqaradi?
43. C2 tizimlarini aniqlash va bloklash usullarini izohlang.
44. C2 tizimlarini tahlil qilishda qaysi vositalardan foydalaniladi?
45. C2 tizimlari bilan bog‘liq hujumlarni cheklash uchun qanday texnologiyalar mavjud?
46. C2 serverni eksploitlash qilish jarayonini tushuntiring.
47. C2 tizimlarining ijtimoiy xavfsizlikka ta’siri haqida yozing.
48. C2 hujumlarining zamonaviy texnikalarini tushuntiring.
49. Oddiy C2 hujumining ishlash prinsipi haqida yozing.
50. C2 tizimlarini himoyalash strategiyalarini tahlil qiling.
51. “Threat Hunting” jarayonining asosiy bosqichlarini tushuntiring.
52. “Threat Hunting” uchun laboratoriyani qanday tashkil qilish mumkin?
53. “Threat Hunting” vositalarining imkoniyatlarini izohlang.
54. “Threat Hunting” strategiyasining samaradorligi nimalarga bog‘liq?
55. “Threat Hunting” laboratoriyasida duch kelinadigan qiyinchiliklarni yozing.
56. Oddiy “log” tahlili orqali tahdidlarni aniqlash jarayonini tushuntiring.
57. Tahdidlarni tahlil qilishda qaysi vositalar samarali hisoblanadi?
58. “Threat Hunting” ning kiberxavfsizlikdagi o‘rni qanday?
59. Tahdidlarni aniqlash uchun qanday algoritmlar ishlatiladi?
60. “Threat Hunting” va eksploitlarni tahlil qilishning o‘zaro bog‘liqligini tushuntiring.
61. Linux eksploitlarini aniqlashda asosiy texnologiyalarni tushuntiring.
62. Windows eksploitlariga qarshi samarali himoya texnologiyalari qanday?
63. Kernel darajasida xavfsizlikni oshirish usullarini izohlang.
64. Xavfsizlik texnologiyalarining eksploitlarga qarshi samaradorligini baholang.
65. “ASLR” texnologiyasining afzalliklari va kamchiliklarini tushuntiring.
66. Exploitlarni aniqlashda xavfsizlikni qanday yaxshilash mumkin?
67. Kernel xavfsizligini ta’minlashda yangi texnologiyalarni taklif qiling.
68. Linux va Windows eksploitlarini aniqlashda asosiy qiyinchiliklarni izohlang.
69. Operatsion tizim xavfsizligi qanday tamoyillarga asoslanadi?
70. O‘z fikringizcha, zamonaviy eksploitlar qanday rivojlanadi?
71. Linux eksploitlari nima va ular qanday maqsadlarda qo'llaniladi, Ushbu eksploitlarni rivojlantirishda asosiy e'tibor nimaga qaratiladi?
72. Kernel eksploitlarini aniqlash va rivojlantirishda qaysi vositalar keng qo'llaniladi, Ushbu vositalar qanday imkoniyatlarni taqdim etadi?
73. Linux operatsion tizimida zaifliklarni tahlil qilish uchun foydalaniladigan asosiy vositalarni sanab bering va ulardan biri ustida qisqacha izoh bering.
74. “Metasploit Framework” eksploit vositasi qanday ishlaydi va linux tizimlaridagi zaifliklarni sinovdan o‘tkazishda qanday rol o‘ynaydi?
75. Sizga linux tizimida o‘rnatilgan zaif xizmatni topish vazifasi yuklatildi, ushbu jarayonda foydalanadigan vositalar va qadamlarni izohlang.
76. “Buffer” toshib ketishi nima va u qanday xatolarga olib kelishi mumkin?
77. “Pointers” nima va ular qanday maqsadda ishlatiladi?
78. C dasturlash tilida “**stack”** va “**heap”** segmentlari orasidagi asosiy farqni tushuntiring.
79. Hujum imkoniyatlari orasida zaif fayl ruxsatlarini aniqlash va umumiy kutubxonani zararli kutubxona bilan almashtirish maqsadida qandaymexanizmidan foydalanish mumkin.
80. Tahdidlarni aniqlash laboratoriyasini yaratish uchun qanday texnologiyalar kerak bo‘ladi va ularning asosiy talablari nimalardan iborat?
81. “DetectionLab” va “HELK” o‘rtasidagi asosiy farqlar qanday va qaysi holatda ularning har birini ishlatish tavsiya etiladi?
82. Bulutda tahdidlarni aniqlash laboratoriyasini yaratishda qanday xavfsizlik va iqtisodiy omillarni hisobga olish kerak?
83. “DetectionLab” ning asosiy vositalari yordamida laboratoriyangizni qanday qilib toʻgʻri boshqarish va qayta yuklash jarayonlarini amalga oshirish mumkin?
84. “HELK” oʻrnatish jarayonida “Docker Compose” konfiguratsiyasining qaysi variantini tanlash kerak va nega ushbu variant laboratoriya maqsadlariga mos keladi?
85. “OSSIM” yordamida ma’lumotlar manbalarini normallashtirish (Normalizing Data Sources with OSSEM).
86. “OSSEM” yordamida ma'lumotlar manbalarini vizualizatsiya qilish.
87. “Stack” operatsiyalari nima?
88. Funksiyalarni chaqirish protseduralari nima?
89. Bufer toshib ketishi nima?
90. Lokal buferni toshdirish eksploitlari qanday ishlaydi?
91. Eksploitni yaratish jarayoni qanday amalga oshiriladi?
92. Metasploit nima?
93. “PowerShell Empire” ning imkoniyatlari.
94. “Covenant” nima?
95. “Covenant”ning ishlash tamoyili.
96. “Covenant”ning imkoniyatlari va qo‘llanilishi.
97. “Dekomplyator” va “dekomplyatsiya” nima?
98. “Ghidrada kod browser” va uning vazifalari.
99. “Gray hat” xakerlik nima?
100. “Bug bounty” zaifliklari va uning ahamiyati.
101. “Black hat hacking” - qora shlyapali xakerlik.
102. “Cyber Kill Chain” nima?
103. “IDA Pro” da xotira xaritasini tahlil qilish uchun qanday vositalar mavjud?
104. “Ghidra” ning vazifasi va qoʻllanilishi.
105. “IDA Pro” dasturida xususiy funktsiyalarni qanday izlash va tahlil qilish mumkin?
106. “IDA Pro” da “Disassembly” va “Decompilation” o‘rtasidagi farqni tushuntirib bering.
107. “IDA Pro” ni ishlatishda “Strings” va “Imports” ma’lumotlarini qanday tahlil qilish mumkin?
108. “IDA Pro” da xotira xaritasini tahlil qilish uchun qanday vositalar mavjud?
109. Tahdid ovining ish jarayoni ketma-ketlikda ayting?
110. “MITRE ATT&CK Framework” haqida ma’lumot bering.