**1-BOB**

**1-Amaliy test**

1. Quyidagilardan qaysi biri passiv razvedka harakati hisoblanadi?

* 1. Mahalliy qog‘ozda qidirish
  2. Inson resurslariga qo‘ng‘iroq qilish
  3. *nmap -sT* buyrugʻi yordamida
  4. O‘rtadagi odam hujumini o‘tkazish
  5. Firibgar qaynoq nuqtasi sozlanmoqda

1. DES algoritmidan keyin maxfiylikni ta’minlashning asosiy usuli sifatida NIST tomonidan qaysi shifrlash tanlangan?
   1. 3DES
   2. Ikki baliq
   3. RC4
   4. AES
2. Qaysi vosita 802.3 muhitiga odam-in-the-middle hujumini o'tkazishga qodir?
   1. Ettercap
   2. Qobil va Hobil
   3. Wireshark
   4. nishoncha bilan oʻchirish
3. An'anaviy xavfsizlik devori va IPS o'rtasidagi farq nima?
   1. Xavfsizlik devorlari jurnallarni yaratmaydi.
   2. IPS paketlarni tashlab bo'lmaydi.
   3. IPS qoidalarga amal qilmaydi.
   4. IPS paketlarni ajratishi mumkin.
4. Nega maqsadli tarmoqni sekin-asta skanerlash muhim?
   1. IDSni ogohlantirishga yo'l qo'ymaslik uchun
   2. Tarmoqni sekin skanerlash kerak emas.
   3. Xavfsizlik devoridan qochish uchun
   4. Xizmatlar boshlanmagan bo'lishi mumkin, shuning uchun asta-sekin boshlash kech boshlangan xizmatlarni qo'lga olishingizni ta'minlaydi.
5. Siz kompaniyangizning IT bo'limida katta menejerisiz. Ijtimoiy muhandislik hujumlarining oldini olishning eng tejamkor usuli nima?
   1. HIDSni o'rnatish.
   2. Barcha yamalar dolzarb ekanligiga ishonch hosil qiling.
   3. Barcha elektron pochta harakatlarini kuzatib boring va nazorat qiling.
   4. Foydalanuvchilarni anglash bo'yicha treninglarni amalga oshiring.
6. Axloqiy xakerlik doirasining qaysi bosqichida jurnal ma'lumotlarini o'zgartirasiz yoki o'chirib tashlaysiz?
   1. Skanerlash va ro'yxatlash
   2. Kirish imkoniyati
   3. Tan olish
   4. Treklarni qoplash
7. Hacker maqsadli ish stantsiyasida quyidagilarni amalga oshirmoqda:

nmap -sT 192.33.10.5. Tajovuzkor qaysi bosqichda?

* 1. Treklarni qoplash
  2. Ro'yxatga olish
  3. Skanerlash va ro'yxatlash
  4. Kirish imkoniyati

1. Qaysi shifrlash algoritmi nosimmetrik oqim shifri?
   1. AES
   2. ECC
   3. RC4
   4. PGP
2. Penetratsiya testini o'tkazishda eng muhim jihat nima?
   1. Rasmiy yozma kelishuv olish
   2. Barcha harakatlar va faoliyatni hujjatlashtirish
   3. Jiddiy tahdidlarni zudlik bilan bartaraf etish
   4. Axborotni ta'minlash guruhi bilan to'g'ri aloqani ta'minlash
3. Siz ulkan texnologik kompaniya uchun CISO. Siz 2017 yilda joriy etiladigan yangi mobil qurilmalaringiz uchun shifrlash shifrini amalga oshirish bilan shug'ullanasiz. Qaysi shifrlash standartini tanlaysiz?
   1. RC4
   2. MD5
   3. ECC
   4. Skipjack
4. SYN skaneri nimani amalga oshiradi?
   1. Bu to'liq TCP ulanishini o'rnatadi.
   2. Bu faqat "yarim ochiq" aloqani o'rnatadi.
   3. Bu maqsad bilan ACK aloqasini ochadi.
   4. Maqsadli tizimdagi barcha yopiq portlarni aniqlaydi.
5. ARP so'rovining asosiy zaifligi nima?
   1. LANdagi barcha xostlarga manzil so'rovini yuboradi.
   2. Manzil foydalanuvchi va maxfiy soʻz bilan ochiq matn koʻrinishida qaytariladi.
   3. Manzil so'rovi DoS-ga olib kelishi mumkin.
   4. Manzil so'rovi tajovuzkorning MAC-manzili bilan buzilishi mumkin.
6. Siz ommabop ijtimoiy veb-sayt uchun CISO. Yaqinda veb-serverlaringiz SSL Heart Bleed nol kunlik ekspluatatsiyasi bilan buzilganligini bilib oldingiz. Qarshi himoya qilish uchun sizning eng ehtimoliy birinchi harakatlaringiz nima bo'ladi?
   1. Barcha tizimlarni yamalang.
   2. Yangi kriptografik kalitlarni yaratish.
   3. Internetga qaraydigan veb-xizmatlar oʻchirib qoʻyildi.
   4. Nozik ma'lumotlarga kirishni cheklash.
7. Hozirda muvaffaqiyatli o'rtadagi odam-in-the-middle hujumini amalga oshirayotgan hujumchi qaysi bosqichda?
   1. Kirish imkoniyati
   2. Kirishni saqlab qolish
   3. Tan olish
   4. Treklarni qoplash
8. Qaysi ekspluatatsiya usuli dushmanga URL ichidagi SQL so'rovlarini sinab ko'rishga imkon beradi?
   1. SQL-in'ektsiya
   2. XSS
   3. Nayzali fishing
   4. Rails qarshi usuli bo'yicha Ruby
9. Microsoft Windows 7 OS uchun standart TTL qiymatlari nima?
   1. 64
   2. 128
   3. 255
   4. 256
10. SQL in'ektsiyasi zaifliklarini baholash va sinovdan o'tkazish uchun qaysi kirish qiymatidan foydalanasiz?
    1. SQL testi
    2. ma'mur va parol
    3. || yoki |!
    4. 1'or'1'='1
11. Xavfsizlik haqida gap ketganda, Telnet bilan SSH-dan foydalanishning salbiy tomoni nimada?
    1. SSH trafik va hisob ma'lumotlarini shifrlaydi.
    2. Koʻrmassan. Albatta, sen oʻshaning nima qilishini koʻrmassan.
    3. Ma'lumotlar aniq ko'rinishda yuboriladi.
    4. Qanday kalitlardan foydalanayotganingizni bilmaysiz.
12. O'lim pingi birinchi marta qaysi yilda paydo bo'ldi?
    1. 1992
    2. 1989
    3. 1990
    4. 1996
13. Quyidagi viruslardan qaysi biri eng yuqumli bo'lgan?
    1. Melisa virusi
    2. Men sizni virusni sevaman
    3. Blue Cross virus punter
    4. Stuxnet
14. Siz yordam xizmati guruhining bir qismisiz. Siz foydalanuvchingizdan kompyuteringiz vaqti-vaqti bilan sekinlashishi haqida chipta olasiz. Foydalanuvchi shuningdek, vaqti-vaqti bilan hujjatlar yo'qolib ketganini yoki asl joyidan boshqasiga ko'chirilganligini ta'kidlaydi. Foydalanuvchi kompyuteriga masofaviy ish stolini tekshirib koʻring. Yangi jarayonlar boshlanganini ko'rish uchun eng ehtimoliy joy qaerda?
    1. Vazifalar boshqaruvchisidagi "Jarayonlar" paneli
    2. C:\temp
    3. Vazifalar boshqaruvchisidagi Loglar paneli
    4. C:\Windows\System32\User
15. Tarmoq muhandisi sifatida siz simsiz aloqa orqali ikkita korporativ ob'ektni bog'lash vazifasini oldingiz. Ushbu ob'ektlar bir-biridan 20 mildan ortiq masofada joylashgan, har bir joyda 400 dan ortiq xodimlarni o'z ichiga oladi va 20,000 AQSh dollari byudjetga ega. Har bir sayt bitta rejimli tolali ulanishga ega. Bo'shliqni ko'paytirish uchun qaysi antennadan foydalanasiz?
    1. Ko'p reymli tolali tolali
    2. Juda kichik diyaframli terminal (VSAT)
    3. Omni yo'nalish antennasi
    4. Yo'nalishli antenna
16. Tekshirish summasi nimani anglatadi?
    1. Ma'lumotlar manziliga yetib kelganini
    2. Uch tomonlama TCP / IP qo'l siqish tugagan
    3. Tranzit yoki dam olish paytida ma'lumotlarda o'zgarishlar bo'lganligi
    4. Ma'lumotlar xotirasidan keyin hajmi
17. Quyidagilardan qaysi biri RSAning ro'yxatdan o'tgan asosiy kuchli tomonlaridan biri?
    1. 1,024 bit
    2. 256 bit
    3. 128 bit
    4. 512 bit
18. E-pochtani rad etishni ta'minlash uchun qaysi algoritmni amalga oshirishni tanlaysiz?
    1. AES
    2. DSA
    3. 3DES
    4. Skipjack
19. Quyidagilardan qaysi biri poyga holatini tasvirlaydi?
    1. Bir vaqtning o'zida ikkita shart ro'y beradi va foydalanuvchining yuqori ruxsatlari bilan o'zboshimchalik bilan buyruqlar bajarilishi mumkin bo'lsa, keyinchalik dushman tomonidan ishlatilishi mumkin
    2. Bu erda ikkita shart bir-birini bekor qiladi va foydalanuvchi imtiyozlari darajasiga qarab o'zboshimchalik bilan buyruqlar ishlatilishi mumkin
    3. Bu yerda bitta foydalanuvchi hisobi uchun ikkita shart bajariladi
    4. Bu yerda ikkita shart yuqori foydalanuvchi imtiyozlari bilan bir vaqtda bajariladi
20. Sizning oxirgi mijozlaringiz tashqi tarmoqdagi biron bir veb-saytga kira olmasliklarini xabar qilishadi. Tarmoq ma'muri sifatida siz ba'zi haqiqatlarni aniqlashga qaror qilasiz. Tekshiruvingiz natijasida siz ularning IP-manzilidan foydalanib, LANdan tashqarida tashqi veb-saytlarga ping qilish imkoniyatiga ega ekanligingizni aniqlaysiz. Domen nomlari o'lchamlari bilan veb-saytlarga ping qilish ishlamaydi. Muammoga nima sabab bo'lishi mumkin?
    1. Xavfsizlik devori DNS piksellar sonini bloklamoqda.
    2. DNS server to'g'ri ishlamaydi.
    3. Tashqi veb-saytlar javob bermayapti.
    4. HTTP GET so'rovi xavfsizlik devoridan chiqib ketishdan tashlanmoqda.
21. Siz mahalliy shahar uchun xavfsizlik ma'muriyatisiz. Siz yangi IPS o'rnatdingiz. Uni ulash va ba'zi asosiy IPS qoidalarini qo'llashdan tashqari, boshqa hech qanday konfiguratsiya amalga oshirilmagan. Ertasi kuni ertalab kelasiz va jurnallarda IPS tomonidan yaratilgan juda ko'p faoliyat borligini aniqlaysiz, shuning uchun ko'rish juda ko'p vaqt talab qiladi. IPSdan jurnallarning katta oqimiga nima sabab bo'lishi mumkin?
    1. Kesish darajasi belgilandi.
    2. Tarmoqda DoS hujumi bo'lgan.
    3. LAN kommutatsiya aylanishini boshdan kechirdi.
    4. Hech qanday baza o'rnatilmagan.
22. Qaysi usul mijoz tomonidagi hujum deb hisoblanadi?
    1. Saytlararo skript (XSS)
    2. O'rtadagi odam hujumi
    3. Sug'orish teshigi hujumi
    4. Xizmatdan bosh tortish (DoS)
23. Penetratsion sinovchi sifatida faqat siz va kompaniyaning bir nechta tanlangan shaxslari sinovdan o'tadigan maqsadli tarmoqni bilib olasiz. Siz shuningdek, kompaniyaning nomi va joylashuvidan tashqari maqsadingiz haqida nol ma'lumotga egasiz. Bu qanday baholash turi deb ataladi?
24. Kulrang qutini sinash
25. Oq qutini sinash
26. Qora qutini sinash
27. Blue box sinov
28. Hujumchi sifatida siz maqsadingizni topdingiz. Keyingi ikki hafta davomida xodimlarning muassasaga kirishini va tashqariga chiqishini kuzatish va kuzatish bilan shug'ullanasiz. Shuningdek, old stol etkazib berilgan katta paketlarni, shuningdek, kirish nishonlari bo'lmagan odamlarni qanday ishlashini kuzatasiz. Nihoyat siz o'tkazilayotganini ko'rgan xavfsizlik patrullarining mustahkam jadvalini tuzasiz. Siz nima qilyapsiz?
    1. Moʻljalning kattaligi
    2. Kirish imkoniyati
    3. Kirishni saqlab qolish
    4. Tan olish
29. Qaysi skanerlash vositasi hacker uchun aniq natijalarni beradi?
    1. NCAT
    2. nishoncha bilan oʻchirish
    3. Ping
    4. Nslookup
30. Nima uchun tajovuzkor Ncat yordamida ochiq TCP ulanish tekshiruvini o'tkazishi

kerak?

* 1. Tajovuzkor tizimga hujum qilishni xohlamaydi.
  2. Tajovuzkor nmap funktsiyasidan foydalangan holda xato qildi.
  3. Tajovuzkor tarmoq xizmatlariga ulanishga harakat qilmoqda.
  4. Tajovuzkor ulanish uchun qanday portlar ochiq ekanligini ko'rishga harakat qilmoqda.

1. Nima uchun tajovuzkor optik tolali liniyaga kirishdan qochishni xohlaydi?
   1. Tolali liniyaga kirish juda ko'p pul sarflanadi.
   2. Agar noto'g'ri bajarilsa, u butun ulanish signalining pasayishiga olib kelishi mumkin, shuning uchun maqsadli tashkilotning istalmagan e'tiborini jalb qiladi.
   3. Tarmoq trafigi sezilarli darajada sekinlashadi.
   4. Liniyaga tegish IPS / IDS-ni ogohlantirishi mumkin.
2. Siz maqsadingizning veb-serveriga muvaffaqiyatli kirgan tajovuzkorsiz. Siz maqsadli tashkilotning veb-saytida veb-saytni buzdingiz va ma'muriy imtiyozlar bilan o'zingizning hisob ma'lumotlaringizni yaratishingiz mumkin. Ma'lumotlarni eksfiltratsiyadan oldin keyingi harakat nima?
   1. Siz yaratgan yangi foydalanuvchi hisobiga kiring.
   2. Orqaga qayting va jurnallarni o'chirib tashlang yoki tahrirlang.
   3. Seansdan chiqishingizga ishonch hosil qiling.
   4. Boshqa sessiyaga ko'chib o'tganingizga ishonch hosil qiling va tizimdan chiqing.
3. Kerberosdan foydalanishning asosiy kamchiligi nima?
   1. Nosimmetrik kalitlar xavfsiz bo'lmasa, buzilishi mumkin.
   2. Kerberos zaif kriptografiyadan foydalanadi va kalitlarni osongina buzish mumkin.
   3. Kerberos assimetrik kriptografiyadan foydalanadi va uni osongina ishlatish mumkin.
   4. Dushman tizimga yoki xizmatga kirish uchun chipta berish chiptasini qayta ijro etishi mumkin.
4. Windows tizimidagi maxfiy soʻz fayli qayerda joylashgan?
   1. C:\Windows\temp
   2. C:\Win\system\config
   3. C: \ Windows \ accounts \ config
   4. C:\Windows\system32\config
5. Agar dushman XMAS tekshiruvini o'tkazsa, yopiq portlarda qanday javob oladi?
   1. RST
   2. RST/ACK
   3. Javob yoʻq
   4. FIN/ACK
6. Nima uchun dushman o'z yukini maqsadli qurbonga yuborishdan oldin kodlashi kerak?
   1. Foydali yukni kodlash qo'shimcha foyda bermaydi.
   2. Foydali yukni kodlash orqali dushman aslida foydali yukni shifrlaydi.
   3. Kodlangan foydali yuk xavfsizlik devorini chetlab o'tishi mumkin, chunki foydali yuk bilan bog'liq port yo'q.
   4. Yukni kodlash IPS / IDS aniqlashni chetlab o'tishi mumkin, chunki u imzoni o'zgartiradi.
7. Qaysi maxfiy soʻz xavfsizroq?
   1. !9Apple
   2. pass123!!
   3. P@$$w 0rD
   4. keepyourpasswordsecuretoyourself
8. Quyida keltirilganlardan qaysi biri DNS zaharlanishini yaxshiroq ta'riflaydi?
   1. Dushman qurbonlarning MAC manzilini o'zlari bilan almashtiradi va almashtiradi.
   2. Dushman ularning zararli IP-manzilini jabrlanuvchining domen nomi uchun IP-manzili bilan almashtiradi.
   3. Dushman qonuniy domen nomini zararli domen nomi bilan almashtiradi.
   4. Dushman domen nomiga moslangan qonuniy IP-manzilni zararli IP-manzil bilan almashtiradi.
9. Quyidagilardan qaysi biri dushmanga autentifikatsiya qilish uchun sertifikatlarni qalbakilashtirishga imkon beradi?
   1. Wireshark
   2. Ettercap
   3. Qobil va Hobil
   4. NCAT
10. WEPda qaysi shifrlash standarti qo'llaniladi?
    1. AES
    2. RC5
    3. MD5
    4. RC4
11. Siz ofisingizning ichida o'tiryapsiz va avtoturargohda noutbukga ulangan baland antennaga o'xshash narsa bilan g'alati odamni ko'rasiz. Begona odam nima qilishi mumkin?
    1. O'zlarining shaxsiy elektron qurilmalarini qo'pol ravishda kuchaytirish
    2. Urush haydash
    3. Jangchi
    4. Bluesnarfing
12. Tarmoq ma'muri sifatida siz eshittirish manziliga ping yuboradigan tanish IP- manzilni ko'rasiz. Nima sodir bo'layotganiga ishonasiz?
    1. Smurf hujumi
    2. DNS bilan zaharlanish
    3. O'rtadagi odam hujumi
    4. Gatewayni yuqtiruvchi troyan virusi
13. Qaysi biri xizmatdan bosh tortishni (DoS) yaxshiroq ta'riflaydi?
    1. Jabrlanuvchining kompyuterida virus yuqtirilgan.
    2. Noto'g'ri tuzilgan kalit kommutatsiya aylanmasida.
    3. Dushman sertifikatni soxtalashtirmoqda.
    4. Dushman veb-serverda iloji boricha ko'proq "yarim ochiq" ulanishlarni ochib, maqsadli tizimning barcha mavjud xotirasini iste'mol qilmoqda.
14. Windows SAM faylida, qaysi atributlar dushmanga berilgan hisob administrator hisobi ekanligini ko'rsatadi?
    1. 500
    2. 1001
    3. ADM
    4. ADMIN\_500
15. Shimoliy va Janubiy Amerika uchun qaysi mintaqaviy Internet registri javobgar?
    1. PISHGAN
    2. AMERNIC
    3. Laknik
    4. ARIN
16. Quyidagi harakatlardan qaysi biri maqsadni skanerlashda so'nggi qadamdir?
    1. Zaifliklarni skanerlang.
    2. Jonli tizimlarni aniqlang.
    3. Ochiq portlarni kashf eting.
    4. Operatsion tizim va serverlarni aniqlang.
17. Quyidagilardan qaysi biri ICMP Type 8 kodini eng yaxshi ta'riflaydi?
    1. Uskuna filtrlanmoqda
    2. Tarmoq yoʻnalishi notoʻgʻri yoki mavjud emas
    3. Echo soʻrovi
    4. Moʻljallangan manzilga etib boʻlmaydi
18. Quyidagi parametrlardan qaysi biri yaxshi tanilgan portlarni koʻrsatadi?
    1. 0 uchun 1023
    2. 0 uchun 255
    3. 1024 uchun 49151
    4. 1 dan 128 gacha
19. Urush terish nima?
    1. Modemda DoS-ni olib borayotgan dushman
    2. Qaysi modemlar ochiq ekanligini koʻrish uchun dushman terilmoqda
    3. Modemni yovuz egizak sifatida ishlatadigan dushman
    4. Yopiq modemlarni tekshiruvchi dushman
20. Nmap buyrug'i uchun quyidagi kalitlardan qaysi biri operatsion tizimni izlaydi?
    1. -sO
    2. -sFRU
    3. -A
    4. -sX
21. Windows-dagi buyruq satri interfeysidan foydalanib, domen ichidagi barcha tizimlarni ko'rsatish uchun dushman qanday buyruqdan foydalanadi?
    1. netstat -R /domen
    2. Aniq koʻrinish /<domain\_name>:d omain
    3. aniq ko'rinish /domen:<domain\_name>
    4. netstat /domen:<domain\_name>
22. Siz aeroport terminalida yo'lovchisiz. Siz terminalga qaraysiz va planshetidan foydalanayotgan yosh ayolning yelkasiga qaragan odamni ko'rasiz. U nima qilyapti deb o'ylaysiz?
    1. Urush haydash
    2. Yelkada bemaqsad qilish
    3. Urush yelkasi
    4. Yelka kriko
23. Siz maqsadli saytda SQL in'ektsiyasi zaifliklarini baholashni muvaffaqiyatli o'tkazgan tajovuzkorsiz. SQL in'ektsiyasi qismi sifatida o'zingizning zararli ma'lumotlar bazangiz bilan maqsadli ma'lumotlar bazasini qo'shish uchun qaysi kalit so'zni ishlatasiz?
    1. ITTIFOQ
    2. QO'SHISH
    3. TANLASH
    4. QOʻSHILISH
24. Qaysi parametr xotiradagi ma'lumotlarning bir qismiga kodni in'ektsiya qilish kontseptsiyasini tasvirlaydi, bu esa abritar buyruqlarni bajarishga imkon beradi?
    1. Bufer toʻldirish
    2. Halokat
    3. Xotiradan toʻlib-toshma
    4. Ma'lumotlar toshqini
25. Quyidagi usullardan qaysi biri aloqani tashabbuskor qilish va o'rnatish orqali tashqi tarmoq va xususiy tarmoq o'rtasida vositachi vazifasini bajaradi?
    1. Proksi-server
    2. Xavfsizlik devori
    3. yo'naltirgich
    4. Oʻzgartirish
26. Tajovuzkor sifatida siz o'chirib qo'yilishi kerak bo'lgan xizmatdan foydalangan holda maqsadingizdan muvaffaqiyatli foydalandingiz. Xizmatda siz qulaylik bilan foydalanishingiz mumkin bo'lgan zaifliklar mavjud edi. Bu erda nima bo'lishi mumkin?
    1. Administrator to'g'ri yamalarni qo'llamadi.
    2. Veb-server noto'g'ri sozlangan.
    3. Siz asal bilan shug'ullanyapsiz.
    4. Xavfsizlik devori toʻgʻri moslanmagan.
27. Linux tizimida kirgan oxirgi foydalanuvchining faoliyati bilan bog'liq bo'lgan log fayli qani?
    1. /var/log/user\_log
    2. /var/log/xabarlar
    3. /war/people/lustlog
    4. /var/log/last\_user
28. SSH qaysi standart portdan foydalanadi?
    1. Port 22
    2. Port 21
    3. Port 443
    4. Port 25
29. Pentester sifatida siz mijozingiz uchun tizimlar guruhida baholash uchun yollanasiz. Sizga muhim aktivlar ro'yxati, domen kontrolleri ro'yxati va virtual shareddlar ro'yxati taqdim etiladi. Boshqa hech narsa taqdim etilmadi. Siz qanday turdagi sinovlarni o'tkazyapsiz?
    1. Oq shlyapa sinovlari
    2. Kulrang shlyapa sinovi
    3. Kulrang qutini sinash
    4. Qizil shlyapa sinovlari
30. Quyidagilardan qaysi biri olov yurish *atamasi nimani* anglatishini eng yaxshi tasvirlaydi?
    1. TTL qiymatini xavfsizlik devori 1 tomonidan kamaytirish, port ochilishini ko'rsatadi.
    2. Ping toshqini bilan xavfsizlik devorida xizmatdan bosh tortishga sabab bo'ladi
    3. Xavfsizlik devorida ping tekshiruvini o'tkazish
    4. TTLni sozlash qaysi serverlar va boshqa hostlarning mavjudligini aniqlash uchun yo'riqnoma o'tkazdi
31. 3-qatlamni skanerlash va ro'yxatga olishni amalga oshirish uchun qaysi vositadan foydalanish mumkin?
    1. Qobil va Hobil
    2. Yahyo ripper
    3. Ping-eater
    4. nishoncha bilan oʻchirish
32. IP protokoli bilan qanday port raqami yoki raqamlar bog'liq?
    1. 0 uchun 65535
    2. Portlar yoʻq
    3. 53
    4. 80
33. Qaysi ikkita protokol aloqasiz?
    1. IP va TCP
    2. IP va FTP
    3. IP va UDP
    4. TCP va UDP
34. Tizimni ruxsat bilan so'roq qiladigan shaxsning roli qanday?
    1. Oq shlyapa
    2. Kulrang shlyapa
    3. Qora shlyapa
    4. Qizil shlyapa
35. Patch boshqaruvi nima?
    1. Mavjud bo'lganda yamalarni tarqatish
    2. Yamalarni ishlab chiqarish muhitiga joylashtirilishidan oldin sinov muhitida sinovdan o'tkazish
    3. Oy oxirida yamalarni tarqatish
    4. Sizning tarmog'ingizda hozirda qanday zaifliklar mavjudligini aniqlash va tahdidni bartaraf etish uchun darhol yamalarni joylashtirish
36. FTP OSI modelining qaysi qatlamida joylashgan?
    1. Seans
    2. Dastur
    3. Tarmoq
    4. Transport
37. Qaysi ekspluatatsiya yurak qon ketishi xuruji bilan bog'liq?
    1. Bufer toʻldirish
    2. O'rtadagi odam
    3. Fraggle-hujum
    4. Smurf hujumi
38. Nmap'dagi qaysi kalit XMAS skanerini chaqiradi?
    1. -sX
    2. -sS
    3. -xS
    4. -sT
39. Quyidagilardan qaysi biri barmoq izi skanerini yaxshiroq ta'riflaydi?
    1. Zaifliklarni qidirish
    2. Nmap uchun -sX kalitidan foydalanish
    3. Skanerdan maʼlumot bazasiga mos xususiyatlar
    4. Yong'in bilan qanday portlar ochilganligini tekshiring
40. Qaysi variant veb-ilovalarni maqsad qilib olgan mijoz tomonidagi hujumni tasvirlaydi?
    1. SQL-in'ektsiya
    2. O'zaro faoliyat saytlarida zararli dasturlarni yuborish
    3. Saytlararo skript yaratish
    4. SQL sayt skripti
41. DNS orqali qaysi portdan foydalaniladi?
    1. 80
    2. 8080
    3. 53
    4. 25
42. Linux-da, qaysi fayl to'liq ism, telefon kabi foydalanuvchi ma'lumotlarini ko'rishga imkon beradi

Raqam va ofis haqida maʼlumot?

* 1. soya fayli
  2. passwd fayli
  3. foydalanuvchima'lumot fayli
  4. foydalanuvchiaccount fayli

1. Paket analizatorida FIN bayrog'i qaerda o'rnatilganligini qaerdan ko'rishingiz mumkin?
   1. TCP – sarlavha
   2. TCP - PaketStencils
   3. UDP – Bayroqlar
   4. Bayroqlar
2. DoS hujumini yaratish uchun fraggle hujumi qaysi turdagi paketdan foydalanadi?
   1. TCP
   2. IP
   3. ICMP
   4. UDP
3. NOP (ishlamaydigan protsedura) ni chaqirish uchun qaysi ko'rsatma qiymati ishlatiladi?
   1. 0x99
   2. 0x91
   3. 0xGH
   4. 0x90
4. Bannerlarni olish uchun qanday protokoldan foydalanasiz?
   1. FTP
   2. Qo'shimcha yordamchi dastur
   3. DNS
   4. Telnet
5. IPv6 ichida quyidagi funktsiyalardan qaysi biri endi ishlamaydi?
   1. ko'p manzilli
   2. Har qanday cast
   3. Unicast
   4. Translyatsiya qilish
6. Muayyan konfiguratsiyalar va hujjatning bosqichma-bosqich ko'rsatmalari bilan serverni o'rnatganingizda nima yaratasiz?
   1. Baza chizig'i
   2. Jarayon
   3. Texnik maslahat
   4. Koʻrsatma
7. Dastur ikkita portdan foydalanadi?
   1. Telnet
   2. ICMP
   3. HTTPS
   4. FTP
8. Quyidagi protokollardan qaysi biri vaqti-vaqti bilan mijoz va serverni o'zaro autentifikatsiya qilish uchun bir-birlariga qarshi chiqishga majbur qiladi?
   1. CHAP
   2. OVOZ CHIQARUVCHI
   3. PAP
   4. PPE
9. Quyidagilardan qaysi biri hisobni boshqarishning hayot aylanishiga kiradi?
   1. Hisob qaydnomasini yaratish
   2. Murojaat rad etildi
   3. Foydalanuvchi autentifikatsiya qilish
   4. Yuqoridagilarning hech biri
10. Quyidagi harakatlardan qaysi biri nozik ma'lumotni qidirib axlat konteynerini qidirib yurgan odamning harakatini tasvirlaydi?
    1. Axlatdan sakrash
    2. Dumpster partiyasi
    3. Axlat sho'ng'ishi
    4. Dumpster sho'ng'ishi
11. Veb-serverga ulanish uchun qanday ikkita umumiy port ishlatiladi?
    1. 80 va 25
    2. 80 va 8080
    3. 443 va 53
    4. 20 va 21
12. Mahalliy saqlash va uchinchi tomon bulutli saqlash xavflarini ko'rib chiqayotganda, qaysi bayonot eng to'g'ri?
    1. Bulutli saqlash yanada xavfsizroq, chunki tijorat sotuvchisi xavfsizlik bo'yicha mutaxassislarni o'qitdi.
    2. Saqlash mahalliy bo'lsa, siz saqlash xizmatlari uchun javobgar va javobgar bo'lasiz.
    3. Siz bulut provayderini zarar uchun sudga berishingiz mumkin.
    4. Bulutda an'anaviy mahalliy saqlash infratuzilmasiga qaraganda ko'proq xavfsizlik qatlamlari mavjud.
13. Port raqami bilan birlashtirilgan IP-manzilni nima deb ataysiz?
    1. TCP/IP
    2. Ulanishga asoslangan protokol
    3. TCP/IP soketi
    4. Soket
14. Tasniflash yorlig'i quyidagilardan qaysi biri bilan bog'liq?
    1. Mavzu
    2. Fayl
    3. Obʼekt
    4. Jild
15. Quyidagi vositalardan qaysi biri rasmiy ravishda CA tomonidan imzolanmagan sertifikatlarni yaratishga imkon beradi?
    1. Qobil va Hobil
    2. nishoncha bilan oʻchirish
    3. Ettercap
    4. Qorong'i eter
16. RAID moslamasining qaysi biri ishlamaydi yoki endi ishlatilmaydi?
    1. RAID-1
    2. RAID-3
    3. RAID-5
    4. RAID-2
17. Ushbu protokol autentifikatsiya qilish maqsadida ishlatiladi; U aniq matnli foydalanuvchi nomlari va parollarni shifrlash shakllari yoki qiyinchilik vositasisiz yuboradi. Bu tasdiqlash protokoli nima?
    1. CHAP
    2. OVOZ CHIQARUVCHI
    3. PAP
    4. MSCHAP
18. "Biror narsa" qaysi autentifikatsiya omili turining bir qismi hisoblanadi?
    1. 1-tur
    2. 3-tur
    3. 2-tur
    4. Ko'p faktorli autentifikatsiya qilish
19. Ikki yoki undan ortiq autentifikatsiya usuli qo'llanilsa, u chaqiriladi?
    1. ko'p bosqichli autentifikatsiya faktori
    2. Ko'p faktorli autentifikatsiya qilish
    3. Ko'p sonli faktorli autentifikatsiya qilish
    4. Multiauthentication faktori
20. Quyidagilardan qaysi biri bilan bog'liq bo'lmagan kalit?
    1. MD5
    2. AES
    3. Skipjack
    4. PGP
21. Qaysi operatsion tizim tuzilishi tarmoq mudofaasi uchun vositalar to'plamini taqdim etadi?
    1. Kali Linux
    2. Windows Server 2012 R2
    3. FreeBSD
    4. Xavfsizlik piyozi
22. Qaysi operatsion tizim tuzilishi tarmoq hujumi (maqsadingizga hujum qilish) maqsadlar uchun vositalar to'plamini taqdim etadi?
    1. Kali Linux
    2. Windows Server 2012 R2
    3. FreeBSD
    4. Xavfsizlik piyozi
23. Antivirus dasturining asosiy kamchiligi nimada?
    1. Bu juda sekin bo'lishi mumkin.
    2. U virusning eng so'nggi ta'riflariga ega bo'lishi kerak.
    3. Ko'plab xost resurslarini talab qilishi mumkin.
    4. Buni boshqarish uchun ko'p harakat talab etiladi.
24. Tarmoqni himoya qilish uchun IDS / IPS echimini amalga oshirish uchun quyidagi dasturlardan qaysi birini ishlatasiz?
    1. Kali Linux
    2. Windows Vista
    3. NCAT
    4. Mirkat
25. UDP paketi uchun maksimal bayt hajmi qancha?
    1. 65,535
    2. 65,507
    3. 1,500
    4. 65,527
26. Hujumchi sifatida, razvedka bosqichida maqsadingizning oyoq izini shakllantirish uchun birinchi bo'lib quyidagi manbalardan qaysi birini boshlaysiz?
    1. –sO kaliti bilan nmap
    2. Kali Linux
    3. Gazetadagi yordam qidirilmoqda bo'limi
    4. Vakolatli foydalanuvchi sifatida yordam xizmatiga qo'ng'iroq qilish
27. FIN bayrog'i o'rnatilgan paketni yuborishda, port ochiq bo'lsa, maqsad nima bilan javob beradi?
    1. RST qaytariladi.
    2. Javob qaytarilmaydi.
    3. RST / ACK qaytariladi.
    4. SYN/ACK qaytariladi.
28. Kommutatsiyada MAC toshqinini o'tkazishning natijasi qanday?
    1. Kalit javob bermaydi.
    2. Bu DoSni yaratadi.
    3. Kalit xuddi markaziy kabi ishlaydi.
    4. Kalit odatdagidek ishlashda davom etadi.
29. Wireshark-da ma'lum bir IP-manzilni qidirish uchun quyidagilardan qaysi biri to'g'ri yo'l?
    1. ip.addr = 192.168.1.100
    2. ip == 192.168.1.100
    3. ip = 192.168.1.199
    4. ip.addr == 192.168.1.100
30. Quyidagilardan qaysi biri 2-turdagi kirishni boshqarish usuli?
    1. Barmoq izi
    2. PIN-kod
    3. GPS manzili
    4. Token kirish kartasi
31. Qaysi turdagi hujum quyidagi vaziyatni eng yaxshi belgilaydi? E-pochtada "Kruizingiz bilan tabriklaymiz!" mavzusi bilan havola mavjud. E-pochta o'quvchiga kruizni talab qilish uchun giperhavolani bosishni buyuradi. Havolani bosganda, o'quvchiga onlayn shaklda ism, ijtimoiy sug'urta raqami va tug'ilgan sana kabi bir qator savollar beriladi.
    1. E-pochta orqali phishing
    2. Nayzali fishing
    3. Ijtimoiy injiniring
    4. Shaxsni o'g'irlash
32. Maqsadli tizimda DDoS-ni bajarish uchun ishlatiladigan zombi kompyuterlar tarmog'i chaqiriladimi?
    1. Botnet
    2. Balchiq ovlash
    3. Ijtimoiy injiniring
    4. To'g'rilar doir
33. Shifrlangan qulflar, mantraplar va bollardlar nima deb hisoblanadi?
    1. jismoniy nazorat qilish
    2. Texnik nazorat qilish
    3. Atrof-muhitni loyihalash orqali jinoyatchilikning oldini olish
    4. Jismoniy to'siqlar
34. Quyidagilardan qaysi biri X.509 standartini tavsiflaydi?
    1. U LDAP tuzilishini belgilaydi.
    2. Bu nosimmetrik shifrlash algoritmi.
    3. Xavfsizlik uchun qum qutisi usulidan foydalanadi.
    4. Unda raqamli sertifikat yaratish standarti tasvirlangan.
35. Quyidagilardan qaysi biri steganografiyani eng yaxshi ta'riflaydi?
    1. Nosimmetrik shifrlash algoritmiName
    2. Sizning shaxsiy kalitingizdan foydalanishga ruxsat berish
    3. Rasmdagi ma'lumotni yashirish yoki uni audio formatda yashirish
    4. Almashtirish va almashtirish yordamida maʼlumotlarni shifrlash
36. Ko'p hollarda quyidagi tasniflardan qaysi biri asal bo'ladi?
    1. Jalb qilish
    2. Tuzoq qilish
    3. Ijtimoiy injiniring
    4. Asal
37. 802.11a kirish nuqtasi qaysi tarmoqli kengligida ishlaydi?
    1. 54 Mbit / s
    2. 1 Gb / s
    3. 5 GHz
    4. 2.4 GHz
38. CEH imtihonining boshqaruv kengashi nima?
    1. (ISC)2
    2. Evropa Kengashi
    3. CompTIA
    4. Microsoft
39. DHCP qaysi transport qatlami protokoli bilan ishlaydi?
    1. IP
    2. TCP
    3. ICMP
    4. UDP
40. Diagrammaga ko'ra, IANA ID nima?
    1. 292
    2. 94089
    3. AQSh
    4. 4083493300
41. Quyidagi skrinshotga ko'ra, Terminal qanday jarayonni identifikatsiyalashda ishlaydi?
42. 1
43. 708
44. 243
45. 1186
46. Quyidagi rasmda ko'rsatilganidek, qanday hujum turi amalga oshirilmoqda?
    1. Zarbalar
    2. DDoS
    3. To'g'rilar doir
    4. Bot hujumi
47. Bu erda ko'rsatilgan uch tomonlama qo'l siqishni yakunlash uchun nima etishmayapti?
    1. ACK/SYN
    2. ACK
    3. TCP/IP
    4. SYN/ACK
48. Quyidagi skrinshotda qaysi jarayon 386 MB xotira oladi

kompyuter?

* 1. Firefox
  2. kernel\_task
  3. Finder
  4. Oyna serveri

1. Quyidagi rasmda qanday hujum turi ko'rsatilgan?
   1. O'rtadagi odam
   2. To'g'rilar doir
   3. DDoS
   4. Nayzali fishing
2. Qaysi skanerda eng ko'p portlar skanerlangan?
   1. Ping
   2. SYN yashirincha
   3. SIND
   4. DUP
3. Quyidagi ekran tasvirida ko'rsatilganidek, foydalanuvchi parolini xash uchun qanday algoritm ishlatilgan?
   1. SHA-512
   2. Kerberos
   3. AES
   4. SHA-256
4. Qaysi fayl yoki dasturda 644 bilan ruxsatnoma o'rnatilgan?
   1. AQSh dollari
   2. aniq
   3. Hajmi
   4. Installer.failurerequests
5. Wireshark pcap faylida berilgan ma'lumotlardan, veb-serverga ulanadigan manba qaysi operatsion tizim?
   1. OS X
   2. Microsoft
   3. Linux
   4. RaspbiyaName

**2-BOB**

**Amaliy test 2**

1.Quyidagilardan qaysi biri ma'muriy nazorat hisoblanadi?

* 1. biometrik qurilma
  2. Mantrap
  3. Xavfsizlik siyosati
  4. Kirish boshqaruvi ro'yxati

1. C sinfidagi tarmoqda, tarmoq ma'murlari subnet niqobi /27-dan foydalanayotgan bo'lsalar, qancha tarmoqni rejalashtirishlari mumkin?
   1. 8
   2. 32
   3. 16
   4. 1
2. Telnet uchun standart port raqami nima?
   1. 21
   2. 23
   3. 53
   4. 443
3. Wiley ASCII matnini oʻn oltiburchak formatga aylantirish.
   1. 57 69 6c 65 79
   2. 63 f3 1i 79 51 ab
   3. 11 Fe A5 6C 81 3h
   4. 87 105 105 101 121 132
4. Qaysi algoritm yaxlitlik yoki maxfiylikni ta'minlamaydi?
   1. DSA
   2. AES
   3. RC4
   4. PGP
5. Quyidagi qisqartmalardan qaysi biri Shimoliy Amerika IP makonini boshqaruvchi institutni anglatadi?
   1. ICANN
   2. PIR-TAHRIR
   3. ARIN
   4. APNIC
6. ARP OSI modelining qaysi qatlamida joylashgan?
   1. Namoyish qatlami
   2. Dastur qatlami
   3. Jismoniy qatlam
   4. Tarmoq qatlami
7. Tepaga o'ralgan ustara simli 8 fut balandlikdagi devor qanday o'lchov hisoblanadi?
   1. To'xtatuvchi chora
   2. Profilaktika chorasi
   3. Tuzatish chorasi
   4. Sanoat o'lchovi
8. Quyidagi standartlardan qaysi biri WPA2 kabi simsiz xavfsizlikni ta'riflash va amalga oshirishga havola qiladi?
   1. 802.1x
   2. 802.11ac
   3. 802.11b / g / n
   4. 802.11i
9. Linuxda qaysi ruxsat qiymati o'qish va bajarishga imkon beradi?

A. 5

B. 7

C. 4

D. 1

1. Quyidagilardan qaysi biri DHCP jarayonini to'g'ri tavsiflaydi?
   1. Kashf qilish, taklif qilish, so'rash, tasdiqlash
   2. So'rov, kashf qilish, taklif qilish, tasdiqlash
   3. Taklif qilish, tan olish, so'rash, kashf qilish
   4. Tan olish, taklif qilish, so'rash, kashf qilish
2. AES ichida bitlarda qanday kalit o'lchamlari ishlatiladi?
   1. 64 va 128
   2. 128, 192 va 256
   3. 128 va 256
   4. 256
3. Quyidagilardan qaysi biri mantiqiy bombani tasvirlaydi?
   1. E-pochta ilovasi orqali yetkazib berilgan va ishga tushirilgan zararli kod
   2. Yadro operatsion tizimiga oʻrnatilgan zararkunandalik dasturlar
   3. Vaqt, sana yoki hatto ma'lum bir klaviatura bosilishi kabi muayyan shartlar bajarilmaguncha harakatsiz yotadigan zararli kod va uning foydali yukini bajaradi
   4. O'zboshimchalik bilan kodni bajarish mumkin bo'lgan CPU registrlarini buzadigan zararli dastur
4. Botnetni boshqarish uchun quyidagi dasturlardan qaysi biri asosan ishlatiladi?
   1. Qo'shimcha yordamchi dastur
   2. FTP
   3. El.pochta
   4. veb-server
5. Siz moliyaviy firmangiz uchun jamoa rahbarisiz. Siz kun oxirida barcha hamkasblar stolini tozalash, axlatni bo'shatish, nozik hujjatlarni parchalash va boshqa muhim hujjatlarni tegishli konteynerlarda saqlashlari kerak bo'lgan siyosatni o'rnatasiz. Bunday siyosatning umumiy nomi nima?
   1. Toza xona siyosati
   2. Toza stol siyosati
   3. Sanitariya siyosati
   4. Siyosatni yigʻish
6. Siz o'z ichki tarmog'iga ega bo'lgan tashkilotda ishlaysiz. Ushbu ichki tarmoq geografik jihatdan ajratilgan kompaniyalarning joylariga ham kengaytirildi. Qaerda

bo'lishidan qat'iy nazar, siz hali ham ichki tarmog'ingizga kirishingiz mumkin; ammo, xavfsizlik masalalari tufayli siz Internetdan foydalanishingiz taqiqlangan. Qanday turdagi

Tarmoq sharoitlarini boshdan kechiryapsizmi?

* 1. VPN
  2. Internet
  3. ekstranet
  4. Intranet

1. OSI modelida elektron darajadagi shlyuzlar qaysi qatlamda ishlaydi?
   1. Seansning qatlami
   2. Maʼlumot bogʻlash qatlamiName
   3. Tarmoq qatlami
   4. Yangi qatlam
2. Qaysi zahira usuli faqat biti o'rnatilgan fayllarni arxivlashga nusxalaydi?
   1. Toʻliq
   2. & Chiziqlar
   3. Hisoblangan
   4. Differentsial
3. Maskaradning *yana bir atama nima*?
   1. Doppelganger
   2. Sharpa
   3. Taqlid qilish
   4. Ikki tomonlama shaxs
4. Yadroga o'rnatilgan zararli dasturlarni antivirus va zararli dasturlarga qarshi dasturlar kabi mahsulotlar bilan aniqlash juda qiyin. Ushbu turdagi zararli dasturlarning nomi nima?
   1. Mantiqiy bomba
   2. Rootkit
   3. Vampire tegish
   4. Yong'oq
5. Qattiq disklar uchun shifrlash kalitlarini saqlaydigan anakartda joylashgan qurilma komponenti uchun qanday nom berilgan, dushmanning qattiq diskni olib tashlashiga va boshqa kompyuterda foydalanishiga yo'l qo'ymaydi?
   1. Qattiq diskni shifrlash
   2. Kripto-shrift
   3. asbob-uskunalar xavfsizlik moduliName
   4. Ishonchli platforma moduli
6. Quyidagi parolni buzish usullaridan qaysi biri eng tezkor?
   1. Lugʻatga hujum
   2. Qo'pol kuch
   3. Tug'ilgan kunga hujum
   4. Xeshni teskarisiga moslashtirish
7. Linux-da foydalanuvchi hisobini noyob tarzda aniqlash uchun qanday dizayner ishlatiladi?
   1. gid bilan
   2. SID
   3. UID
   4. PID
8. Nmap-dan foydalanib, qaysi switch buyrug'i UDP ulanishlarining xostni skanerlashini ta'minlaydi?
   1. -sS
   2. -sX
   3. -PT
   4. -sU
9. Quyidagilardan qaysi biri yuqori darajadagi ota-ona domenini ko'rsatadi?
   1. .org
10. Xavfsizlik ma'muri Telnet-dan foydalanganda quyidagilardan qaysi biri foyda beradi?
    1. Trafik aniq yuboriladi.
    2. Maxfiy soʻz kodlanmagan.
    3. Xavfsizlik ma'murlari dushman nima qilayotganini ko'rishlari mumkin.
    4. Xavfsizlik ma'murlari dushman nima qilayotganini ko'ra olmaydi.
11. Siz kino ishlab chiqarish kompaniyasida ishlaydigan xavfsizlik ma'murisiz. Ulardan biri

sizning kundalik vazifalaringiz ogohlantirilganingizda IDS jurnallarini tekshirishdir. Siz juda ko'p to'liq bo'lmagan uch tomonlama qo'l siqishlarni olganingizni payqadingiz va sizning xotira ishlashi veb-serveringizda sezilarli darajada pasayib ketdi va mijozlar juda sekin ulanishlardan shikoyat qilmoqdalar. Haqiqiy muammo nima bo'lishi mumkin?

* 1. To'g'rilar doir
  2. DDoS
  3. Smurf hujumi
  4. SYN flood

1. "Tarmoq noma'lum" xabari qanday xabar turi va kodi hisoblanadi?
   1. Type 3, Code 6
   2. 3 turi, kod 0
   3. 0 kiriting
   4. 5-tur, kod 1
2. Quyidagi chastota rejimlaridan qaysi biri dushman tomonidan shovqin yaratmaslik yoki siqib qo'ymaslik uchun mo'ljallangan?
   1. To'g'ridan-to'g'ri ketma-ketlik tarqalish spektri
   2. Chastotalarni o'zgartirish uchun keng tarqalgan spektr
   3. Ortogonal chastota bo'linishi multiplexing
   4. Vaqtni taqsimlovchi bir nechta erkin foydalanish
3. Xavfsizlik ma'muri sifatida siz DMZ ichidagi serverlaringiz bilan bog'lanishga harakat qilayotgan turli xil IP ulanishlarini tekshirasiz. Bir necha oy oldin sizning serverlaringiz Eronda ro'yxatdan o'tgan IP-dan juda o'xshash hujumlar va tekshiruvlarni olganligini payqadingiz. Bu safar siz Braziliya, Gretsiya, Sudan va Janubiy Afrikadan kelgan IP-lar bilan shunga o'xshash taktikalarni ko'rasiz. Nima deb o'ylaysiz?
   1. Xakerlik guruhi birlashdi.
   2. DMZ-dagi serverlaringiz hackerlar uchun juda jozibador deb topildi.
   3. Hacker proksi-serverdan foydalanmoqda.
   4. Sizda DMZ-da torrent server o'rnatilgan.
4. Quyida keltirilgan veb-saytlardan qaysi biri telefon raqamlari, administratorning elektron pochtasi va hatto domenni ro'yxatga olish organini o'z ichiga olgan veb-sayt haqida bepul ma'lumot beradi?
   1. Nslookup
   2. qazish
   3. Whois.net
   4. Ping
5. RFC 18 haqida nima ahamiyatga ega?
   1. Bu yo'naltirilmaydigan IP-manzillarni bildiradi.
   2. Bu veb-proksi serverlardan foydalanishni bildiradi.
   3. Unda DMZlardan foydalanish tasvirlanadi.
   4. IPsec-dagi autentifikatsiya sarlavhasini qamrab oladi.
6. ICMP echo so'rovi quyidagi turlardan qaysi?
   1. 8-tur
   2. 3-tur, kod 1
   3. 0 kiriting
   4. 5 turi, kod 0
7. HIDS ko'pincha aniqlash uchun qaysi usuldan foydalanadi?
   1. Imzo bazasi
   2. Anomaliya bazasi
   3. Xavfsizlik devori qoidalari
   4. anomaliya
8. Sertifikat soʻrayotganda quyidagilardan qaysi biri foydalanuvchi haqiqiyligini tasdiqlaydi?
   1. Sertifikatlash markazi
   2. Sertifikat bekor qilinganlar roʻyxati
   3. X.509 va Kerberos
   4. Ro'yxatdan o'tkazish organi
9. Hacker shifrlash algoritmini buzishning turli usullaridan foydalanmoqda, masalan, yon kanal hujumlari, chastota tahlili, shuningdek, bitni aylantirish. Hacker nima qilmoqda?
   1. Qo'pol kuchlash
   2. Hisobga olish maʼlumotlarini yorib tashlash
   3. Raqamli sud ekspertizasi
   4. Kriptoanaliz
10. Quyidagilardan qaysi biri to'g'ri XOR chiqishi?
    1. 0 0 = 1
    2. 1 0 = 0
    3. 1 0 = 0
    4. 1 1 = 0
11. Sniff uchun, Ethernet yoki simsiz tarmoqdan ramkalarni tortib olish uchun tarmoq adapteringiz qaysi rejimga sozlanishi kerak?
    1. Aktiv
    2. Fohishaboz
    3. Yashirin
    4. CSMA/CD rejimi
12. WPA2 da qaysi autentifikatsiya protokoli ishlatiladi?
    1. CCMP
    2. 3DES
    3. AES
    4. SAKRASH
13. Siz mahalliy bank uchun IT xavfsizligini nazorat qiluvchi ma'mursiz. Oldingi kundan boshlab jurnallarni ko'rib chiqayotganingizda, sizning mijozlaringizdan bir vaqtning o'zida keladigan veb-serveringizni maqsad qilib olgan UDP paketlarining juda yuqori tezligini payqadingiz. Aybdor nima bo'lishi mumkin?
    1. Smurf hujumi
    2. DDoS
    3. SYN toshqin hujumi
    4. Fraggle-hujum
14. TCP uch tomonlama qo'l siqishning so'nggi bosqichi qaysi?
    1. ACK
    2. SIND
    3. SYN/ACK
    4. Qo'shma Joylar
15. Token - bu tasdiqlash omilining qanday turi?
    1. 1-tur
    2. 2-tur
    3. 3-tur
    4. 4-tur
16. Qora shlyapa sifatida ishlaysiz, siz juda mashhur ijtimoiy media veb-saytini taqlid qiladigan veb-serverni turishga qaror qilasiz. Siz shuningdek, hamkasblaringiz kompyuterlarida xost faylini yangilaydigan skriptni yaratish va bajarishga qaror qilgan norozi xodimsiz. Bu ularning DNS keshini zaharladi. Sizning hamkasblaringiz ertalabki mashg'ulotlarini ushbu mashhur ijtimoiy media veb-saytiga borib, so'ralganda shaxsiy ma'lumotlarini taqdim etishadi. Afsuski, ular uchun ular veb- saytingizga kirmoqdalar va keyinroq foydalanish uchun ularning hisob ma'lumotlarini saqlaysiz. Siz qanday hujum turini o'tkazdingiz?
    1. O'rtadagi odam
    2. Pharming
    3. Nayzali fishing
    4. Phishing
17. XMAS skanerini yoqish uchun ishlatiladigan TCP sarlavhasi uchun bayroq bayti quyidagilardan qaysi?
    1. 00101001
    2. 11001011
    3. 11101000
    4. 00101100
18. Quyidagilardan qaysi biri "yumshoq" boshqaruvni tasvirlaydi?
    1. Foydalanuvchi shartnomasi
    2. Kirish boshqaruvi ro'yxati
    3. Biometriya
    4. Xavfsizlik xizmatchisi
19. Orqa eshik dushmanga qanday imkoniyatlarni beradi?
    1. Orqa eshiklar ma'lumotlar dasturini buzishi mumkin.
    2. Ular TPMdagi kriptografik kalitlarni yo'q qilishadi.
    3. Ular past darajadagi formatlash operatsiyalarini ta'minlaydi.
    4. Ular mijozga masofadan turib kirishni ta'minlaydi.
20. Quyidagilardan qaysi biri elektron autentifikatsiyani amalga oshirishda foydalanish uchun inson ruhiy atributlari to'plamini tasvirlaydi?
    1. Shaxsiy identifikatsiya guvohnomasi
    2. Soch va barmoq izlari
    3. Biometriya
    4. 3 turi nazorat
21. Quyidagilardan qaysi biri yagona nosimmetrik kriptografiya oqimi shifri?
    1. RC6
    2. Zarb balig'i
    3. RC4
    4. ECE
22. Quyida keltirilganlardan qaysi biri rad etmaslikni ta'minlash uchun ikkita hash qiymatini taqqoslaydi?
    1. DSA
    2. ECE
    3. MD5
    4. SHA-1
23. Qora shlyapa sifatida siz foydalanmoqchi bo'lgan savdo markazida WAP-ni aniqlaysiz. Siz WAP dan foydalanayotganini aniqlaysiz. WAP-dan foydalanish uchun qaysi usuldan foydalanasiz?
    1. RC4 bo'lgan shifrlash algoritmi
    2. Ishga tushirish vektori (IV)
    3. Maxfiy soʻz
    4. Foydalanuvchi ismi va maxfiy soʻzi
24. Hujumingizning izlari bosqichini tugatgan oq shlyapa sifatida, siz maqsadingiz haqida ma'lumot to'plash uchun turli vositalarni ishlatib, davom etasiz. Siz portlarda qanday xizmatlar taklif qilinayotganini aniqlay oldingiz. Siz qanday hisoblar mavjudligini ko'rishingiz va turli xil almashish xizmatlarini ham aniqlashga muvaffaq

bo'ldingiz. Qaysi bosqich

Siz ichkarida ishlayotganmisiz?

* 1. Xizmat proksi
  2. Beparvo skanerlash
  3. Barmoq izi
  4. Ro'yxatga olish

1. Nmap-dan foydalanib, ping süpürme va operatsion tizimni aniqlash yordamida 192.168.0.0 / 24 maqsadli subnetini skanerlash uchun to'g'ri buyruq nima?
   1. nmap -sP -O 192.168.0.0/24
   2. nmap -sP -V 192.168.0.0/24
   3. nmap -sT -P 192.168.0.0/24
   4. nmap -ps -o 192.168.0.0/24
2. Quyidagi xizmatlardan qaysi biri 110 portida ro'yxatdan o'tgan?
   1. SNMP
   2. RPC
   3. POP3
   4. LDAP
3. DNS so'rovlarini o'tkazish uchun Unix tizimlarida quyidagilardan qaysi biri mahalliy ravishda o'rnatilgan?
   1. Ping
   2. nishoncha bilan oʻchirish
   3. Nslookup
   4. qazish
4. Quyidagi saytlardan qaysi biri DNS so'rovlari ma'lumotlarini olishda samarali?
5. Bannerlarni tortish uchun quyidagilardan qaysi birini ishlatishingiz mumkin?
   1. Telnet
   2. Ping
   3. Nmap -sP
   4. del \*.\*
6. Penster sifatida umumiy topilmalaringizga qo'shimcha ravishda qanday tarkibni o'z ichiga olishingiz mumkin?
   1. Yamalangan tizimlar ro'yxati
   2. O'chirilgan hisoblar ro'yxati
   3. Aniqlangan zaifliklar ro'yxati
   4. Bekor qilingan sertifikatlar ro'yxati
7. IEEE port bazasida autentifikatsiya qilish nima?
   1. TACACS
   2. Diametri
   3. 802.1x
   4. TACACS+
8. Quyidagi hujumlardan qaysi biri 53-port yoki boshqa UDP portlaridan foydalanib, Windows tizimiga parchalangan UDP paketlarini yuboradi, bu tizimning ishdan chiqishiga olib kelishi mumkin?
   1. Zarbalar
   2. Bonk
   3. Stackni sindirish
   4. Skurf
9. Quyidagilardan qaysi biri ma'lumotlarni buzish va buzish uchun xost yoki insonning o'zaro ta'siriga muhtoj bo'lmagan dastur?
   1. Yong'oq
   2. virus
   3. TroyanName
   4. Zararkunandalik dasturlar
10. Foydalanuvchi tasodifiy paydo bo'lgan pop-up oyna reklamalarini olayotganini xabar qiladi. Foydalanuvchi kompyuterni qayta ishga tushirishga majbur bo'lgan juda ko'p oynalar mavjud bo'lgan paytlar ham bor. Muammo nima bo'lishi mumkin?
    1. Ish stansiyasiga troyan oʻrnatilgan.
    2. Adware o'rnatilgan.
    3. Pop-uplarni yaratadigan veb-sayt hali ham ishlamoqda.
    4. Rootkit o'rnatilgan.
11. Quyidagilardan qaysi biri biznes yoki tashkilotning kiberhujumlarga qarshi himoya qilishi va ularga qarshi turishi mumkin bo'lgan darajasini tasvirlaydi?
    1. Chuqurlikda mudofaa
    2. Xavfsizlik chorasi
    3. Baza chizigʻini moslash
    4. Xavfsizlik holati
12. Yagona kirish (SSO) strategiyasining bir kamchiligi nimada?
    1. Autentifikatsiya qilish uchun yagona muvaffaqiyatsizlik nuqtasini taqdim etadi.
    2. Xavfsizlik siyosati uchun replikatsiya yo'q.
    3. Maxfiy soʻzlar oddiy matn koʻrinishida saqlanadi.
    4. Foydalanuvchi hisoblariga osongina kirish mumkin.
13. Qaerda ekanligingizga bog'liq bo'lgan autentifikatsiya omili nima?
    1. 1-tur
    2. 2-tur
    3. 3-tur
    4. 4-tur
14. Quyidagilardan qaysi biri parollarni oddiy matnda topishning maqbul usuli?
    1. SSH aloqasini ushlab qo'yish
    2. TCP oqimidan keyin
    3. SSL trafigini kesib qo'yish
    4. Jon Ripper yordamida hisobni buzish
15. Kontentga manzillanadigan xotira jadvali nima?
    1. IP manzillar jadvali
    2. NetBIOS nomlarini koʻrish uchun ishlatiladigan jadval
    3. Portlarga tegishli MAC-manzillar jadvali
    4. IP manzillarga bog'langan domen nomlari ro'yxati
16. Qora shlyapa ICMP xabarining qismlarini jabrlanuvchining tizimiga yuboradi. Tizim barcha paketlarni qabul qilganda, ularni qayta yig'adi va keyin ishdan chiqadi. Qaysi hujum bunday xatti-harakatlarga olib keladi?
    1. O'lim pingi
    2. To'g'rilar doir
    3. Fraggle-hujum
    4. ICMP toshqini
17. Quyidagilardan qaysi biri SSO autentifikatsiya standartida nosimmetrik kalitlardan foydalanadi.
    1. KUNAM
    2. Diametri
    3. Kerberos
    4. HIDLAR
18. Shaxsiy IP-manzilni shlyuzdagi umumiy manzilga o'zgartiradigan protokol nima?
    1. NAT
    2. PAT
    3. GNAT
    4. NAT-T
19. Intrussiyani aniqlash tizimlarida qaysi kombinatsiya ishlatiladi?
    1. NIDS va SIDS
    2. HIDS va SIDS
    3. IDS va IPS
    4. HIDLAR VA NIDLAR
20. Siz yong'in sodir bo'lganda media firmasining kutilgan yo'qotishlarini aniqlash vazifasini bajargan xavfsizlik ma'murisiz. Siz firma o'z aktivlarining yarmini yo'qotishni kutishi mumkin deb hisoblaysiz, bu 10 million dollarga teng. Bundan tashqari, yong'in ehtimoli har 10 yilda bir marta ekanligini aniqlaysiz. Yillik yo'qotishni kutish muddati (ALE) qanday?
    1. 500,000 AQSh dollari yo'qotish
    2. $ 1,000,000 yo'qotish
    3. $ 250,000 daromad
    4. $ 250,000 yo'qotish
21. Qaysi federal qonun dam olish va tranzitda tibbiy yozuvlarni ta'minlashni talab qiladi?
    1. Teng tekislik
    2. HIPAA
    3. FISMA
    4. PATRIOT qonuni
22. Hujumchining (qora shlyapa) himoyachiga (potentsial qurbon) nisbatan bir afzalligi nima?
    1. Vaqti
    2. Onlayn xakerlik forumlari
    3. Pul
    4. Metasploit
23. Quyidagilardan qaysi biri simsiz tarmoqda xavfsizlikka kirish bilan bog'liq?
    1. WPA
    2. 802.1x
    3. Radius
    4. TACACS+
24. Quyidagilardan qaysi biri SQL ma'lumotlar bazasidagi Clients jadvalini o'chiradi?
    1. jadval mijozlarini yangilash
    2. \* MIJOZLARDAN TANLANG
    3. JADVAL MIJOZLARINI QOʻYISH
    4. jadval klientlari
25. Maqsadli tizimda yoki tarmoqdagi zaifliklarni tekshirish uchun quyidagi vositalardan qaysi biri ishlatiladi?
    1. Pishqiriq
    2. NCAT
    3. Nessus
    4. Metasploit
26. Xavfsizlik ma'muri sifatida turli korporativ ofislarga ko'prik o'tkazish uchun simsiz tarmoqlardan foydalanish rejalari bilan bog'liq xavfsizlik xavotirlari mavjud. Ushbu idoralarning joylashuvi tufayli an'anaviy ulanishlar iqtisodiy jihatdan taqiqlanadi. Quyidagi antennalardan qaysi biri istalmagan signalni ushlab qolish ehtimolini cheklab, eng yaxshi qamrovni ta'minlaydi?
    1. Omni
    2. Fan
    3. Yagi
    4. Sun'iy yo'ldosh tishxonasi
27. Quyidagi shifrlash usullaridan qaysi biri Phil Zimmerman tomonidan ishlab chiqilgan?
    1. AES
    2. PGP
    3. DES
    4. DEA
28. IPv6 manzillashning qaysi sxemasidan foydalanadi?
    1. 32 bit
    2. 128 bayt
    3. 32 bayt
    4. 128 bit
29. Quyidagilardan qaysi biri zaiflikni eng yaxshi ta'riflaydi?
    1. Potentsial amalga oshirilayotgan tahdid
    2. Qarshi chora mavjud emas
    3. Tahdidli aktyor
    4. Hodisa
30. Kompaniyadagi yangi foydalanuvchiga minimal imtiyozlar to'plami beriladi. Ular lavozimga ko'tarilib, turli lavozimlarga o'tishlari bilan ko'proq imtiyozlarga ega bo'lishda davom etmoqdalar. Bu nima deb nomlanadi?
    1. Ko'lami creep
    2. Mavqeini kesish
    3. Access creep
    4. Imtiyozlar darajasi
31. Tarmoqdagi qurilmani nima deb ataysiz?
    1. Uskuna
    2. KompyuterComment
    3. Svitvitchi
    4. Kirish qurilmasi
32. Jabrlanuvchi haqida yashirincha ma'lumot to'playdigan dasturni nima deb ataysiz?
    1. TroyanName
    2. josus dastur
    3. Zararkunandalik dasturlar
    4. O'g'irlash dasturi
33. Xizmat to'plami identifikatori (SSID) nechta belgini o'z ichiga oladi?
    1. 32
    2. 64
    3. 20
    4. 128
34. Internet kalit almashinuvi (IKE) protokolining maqsadi nima?
    1. Foydalanuvchi maʼlumotlarini uzatish
    2. Foydalanuvchi profillarini toʻplash
    3. Jamoatchilikka kalitlarni tarqatish
    4. Maxfiy kalitlarni almashtirish
35. Biometrikaga kelsak, noto'g'ri rad etish darajasi (FRR) va noto'g'ri qabul qilish darajasi (FAR) teng bo'lsa, bu kesish nimani anglatadi?
    1. O'tish xato darajasi
    2. Xato tenglashtirish
    3. Yigʻindi
    4. O'tish darajasi teng
36. Ma'lum qonuniy dastur kabi ko'rinishga ega bo'lgan dastur, ammo aslida zararli tabiatan qanday zararli dastur hisoblanadi?
    1. josus dastur
    2. Rootkit
    3. reklama dasturlari
    4. TroyanName
37. SFTP qaysi standart portdan foydalanadi?
    1. 20
    2. 21
    3. 22
    4. 20 va 21
38. Quyidagilardan qaysi biri IEEE 802.3 muhitini tasvirlaydi?
    1. CSMA/CD
    2. Simsiz aloqa xavfsizligi
    3. foydalanuvchilar kirish nazorati ro'yxati
    4. Port bazasida autentifikatsiya qilish
39. Siz yuridik firmaning tizim ma'murisiz. Sizga ma'lum bo'lishicha, bir necha foydalanuvchilar ilovalarni ochishda o'zlarining elektron pochta manzillarini kiritganlarida, ularning kompyuterlari pop-up oynasiga ko'ra tizim buzilishini tiklash uchun qo'lda qayta yuklashni talab qiladi. Muammo nima bo'lishi mumkin?
    1. Troyan qatl etildi.
    2. Mantiqiy bomba ishga tushirildi.
    3. Foydalanuvchilar sabr qilmaydilar.
    4. Foydalanuvchilar patch yangilanishining o'rtasida edilar.
40. Quyidagi xizmatlardan qaysi biri TCP porti 389 bilan bog'liq?
    1. LDAP
    2. IMAP
    3. kichik va o'rta biznes
    4. RPC
41. Tizim tayinlangan ochiq va maxsus kalitlar bilan sertifikat yaratadi. Ushbu tizim uni raqamli imzo qo'yadi. Bu tizimning roli nima?
    1. Ro'yxatga olish markazi
    2. Sertifikatlash markazi
    3. Kerberos tizimiStencils
    4. Server/mijoz muhiti
42. Xavfsizlik ma'muri sifatida siz xodimlarning ma'lumotlarga kirishini faqat ma'lum shaxslar bilan cheklashni xohlaysiz. Qanday kirish turini amalga oshirasiz?
    1. Bilish kerak
    2. Imtiyozlarning eng kam darajasi
    3. Mavjudlikni kamaytirish
    4. Shifrlash jarayonini sozlash
43. Microsoft Office va boshqa ofis to'plamlari ilovalari zararli dasturlarning bajarilishi yoki tarqalishining oldini olish uchun o'chirilishi kerak bo'lgan xususiyatga ega. Qaysi xususiyatni o'chirish kerak?
    1. Pochta
    2. FTP-mijoz
    3. Avtomatik yangilash xususiyati
    4. Makros xususiyati
44. Ishonchli kalitlarga ega bo'lish uchun sertifikatlangan tashkilotning nomi nima?
    1. Hukumat xavfsizligi
    2. Issiq sayt
    3. Eskraj
    4. Offsite zaxiralash
45. HTTPS qaysi standart TCP portidan foydalanadi?
    1. 443
    2. 8080
    3. 80
    4. 22
46. Foydalanuvchi resursga bir marta autentifikatsiya qilsa va keyin qayta autentifikatsiya qilmasdan qo'shimcha ilovalarga kirishga ruxsat berilsa, autentifikatsiyaning qaysi shakli ishlatiladi?
    1. Bir marta ro'yxatdan o'tish
    2. Nonce kirish
    3. Kerberos
    4. Yagona kirish
47. Yo'riqnoma nimani ajratadi?
    1. To'qnashuv domenlari
    2. Eshittirish domenlari
    3. Almashtirish
    4. Joʻnatish usullari
48. 0-turi qaysi UDP porti bilan bog'liq?
    1. U 53-port bilan bog'liq.
    2. U barcha port oralig'ini, ya'ni 0 dan 1023 gacha foydalanadi.
    3. ICMP port raqamlari bilan bog'liq emas.
    4. Portlar 0 turi uchun dinamik ravishda ishlab chiqariladi.
49. Quyidagi saqlash texnologiyalaridan qaysi biri eng o'zgaruvchan hisoblanadi?
    1. Qattiq disk
    2. USB flesh-uskunasi
    3. Protsessor keshi
    4. DDR3
50. Windows tizimining maxfiy soʻz fayli quyidagi kataloglardan qaysi birida joylashgan?
    1. C:\System32\Windows\config
    2. \etc\win\config
    3. C: \ System\Windows\config
    4. C:\Windows\System32\config
51. Hisobning har qanday mumkin bo'lgan parol kombinatsiyasini taxmin qilish harakati qanday?
    1. Qo'pol kuch
    2. Xeshni uzatish
    3. Lugʻatga hujum
    4. Ijtimoiy injiniring
52. Linux-dagi egaga, guruhga va boshqalarga ob'ekt uchun o'qish, yozish va bajarish imtiyozlarini berish uchun qanday buyruqdan foydalanasiz?
    1. Chmod 666
    2. Chmod 777
    3. Chmod 7
    4. Chmod 532
53. Linux-da yuklash uchun turli operatsion tizimlar o'rtasida o'tish uchun quyidagilardan qaysi biri ishlatiladi?
    1. Yagona bootloader
    2. Ctrl+S
    3. Grand Unified Bootloader
    4. Ctrl+F4+S
54. Quyidagilardan qaysi biri tizimni penetratsion sinovdan o'tkazish uchun ramka hisoblanadi?
    1. Metasploit
    2. Qobil va Hobil
    3. Nessus
    4. Xavfsizlik piyozi
55. Windows'da faylni bekitish uchun qanday buyruqdan foydalanishingiz mumkin? Javob. +h attrib <fayl nomi>

B. h+ <fayl nomi>

C. Fayl nomi attrib +h

D. attrib +h <fayl nomi>

1. Quyidagilardan qaysi biri to'g'ri MAC manzili?
   1. 00-12-3e-ff-d4-98
   2. 3i-45-fa-90-25-1b
   3. ff-ff-ff-ff-ff-fg
   4. 65-23-ab-cb-a9
2. Paket xavfsizlik devori qurilmasi OSI modelining qaysi qatlamida ishlaydi?
   1. Qatlam 2
   2. Qatlam 4
   3. Qatlam 7
   4. Qatlam 3
3. Qora shlyapa sifatida siz bir qator pastki tarmoqlarni skanerlaysiz va ba'zi xavfsizlik vositalari yo'q bo'lganini aniqlaysiz. Bundan tashqari, noto'g'ri konfiguratsiyaning aniq belgilari yoki tafsilotlarning etishmasligi mavjudligini aniqlaysiz. Ehtimol, ma'mur yangi boshlovchi bo'lishi mumkin va hali ham o'z tarmog'ini qattiqlashtirish bo'yicha arqonlarni o'rganmoqda. Bu erda nima bo'lishi mumkin?
   1. Asal
   2. Asal
   3. Notoʻgʻri moslamalar
   4. Endi ishlatilmayapti pastki tarmoq
4. Zararli dasturlarga qarshi dasturlardan foydalanishning eng katta kamchiligi nima?
   1. Qayta ishlash resurslarini oladi.
   2. Unda viruslarning dolzarb ta'riflari bo'lishi kerak.
   3. Zararli dasturlarga qarshi dasturlar qimmat.
   4. U markaziy yoki mustaqil ravishda boshqarilishi mumkin.
5. DES algoritmining nomi nima?
   1. DEA
   2. DES
   3. Ikki baliq
   4. 3DES
6. Heartbleed dushmanga nima beradi?
   1. Ekspluatatsiya qilingan vaqtda moʻljallangan serverning xotira tarkibi
   2. A Uy do'sti
   3. O'sha paytda dushmanning xotirasi tarkibi
   4. U dushmanga hech qanday ma'lumot bermaydi.
7. Foydalanuvchi Internetdan musiqa faylini yuklab olganligi haqida xabar beradi. Ular faylni ochganlarida, u dasturni o'rnatgandek tuyuldi va keyin foydalanuvchidan qattiq diskini shifrlash uchun kalitni olish uchun PayPal hisobiga $ 500 dollar

to'lovini yuborishni so'rashdi. Foydalanuvchi yo'q

ish stoliga kirish. Muammo nima bo'lishi mumkin?

* 1. Foydalanuvchi yolg'onni boshdan kechirmoqda.
  2. Foydalanuvchi ransomware dasturini yuklab oldi va o'rnatdi.
  3. Foydalanuvchi zararli dasturlarni o'rnatdi.
  4. Foydalanuvchi notoʻgʻri musiqa faylini yuklab oldi.

1. Qaysi Wi-Fi standarti 2.4 va 5 gigagertsli radio diapazoniga va 100 Mbit / s tezlikka ega?
   1. 802.11i
   2. 802.11
   3. 802.b
   4. 802.11n
2. Bu qanday infratuzilmani tasvirlaydi?
   1. PKI
   2. O'rtadagi odam hujumi
   3. Ijtimoiy injiniring
   4. Kerberos muhiti
3. Ushbu diagrammada asosan qaysi turdagi protokol qo'llaniladi?
   1. Translyatsiya qilish
   2. ARP so'rovi
   3. Ping
   4. DHCP ijarasi
4. Quyidagi diagrammadan qaysi IP-manzilni aniqlay olasiz?
   1. 192.168.1.255
   2. 192.168.1.118
   3. 255.255.255.255
   4. 192.168.1.1
5. Ekran tasvirida qanday kodlash turi qoʻllaniladi?
   1. ASCII
   2. Oltilik
   3. Binar format
   4. UTF-8
6. Quyidagi ekran tasvirida qanday TLS versiyasini topish mumkin?
   1. 1.2
   2. 1.3
   3. 312
   4. 1
7. Quyidagi diagrammada dushman nima qilishga harakat qilmoqda?
   1. O'lim pingi
   2. Veb-serverni aniqlash
   3. SQL-in'ektsiya
   4. Internetni buzish
8. Quyidagi ekran tasvirida ko'rinib turganidek, dushman veb-brauzerdagi URL satrida nima qilishga harakat qilmoqda?
   1. Imtiyozlar darajasi
   2. Katalogni oʻzgartirish
   3. Yashirin SQL in'ektsiyasi
   4. SQL bilan jadvalni oʻchirish
9. Keyingi skrinshotda mijoz qaysi DNS tizimni so'rov qilyapti?
   1. Google Google
   2. Port 53
   3. Port 64234
   4. Yoʻq
10. Quyidagi skrinshotga muvofiq root-ning foydalanuvchisi uchun maxfiy soʻz nima?
    1. ildiz
    2. x
    3. Maxfiy soʻz yoʻq.
    4. x: 0:0
11. Snort-dagi quyidagi logga asoslanib, fayl yuklab olinadigan manzilli port nima?
    1. 56209
    2. 23
    3. 49190
    4. Port mavjud emas.
12. Quyidagilardan qaysi biri foydalanuvchi hisobi hisoblanadi?
    1. usbmux
    2. nur
    3. ossecr
    4. hech kim