Pentest qo’llanma(1 son)

2024
Securesecuz kanali uchun

1. Pentest nima?
2. Pentestni amalga oshirish qanday bosqichlardan iborat?
3. Pentester bo'lishni xohlaysizmi?
4. Dasturlash tillari
5. Kontent menedjerlar (CMS)
6. Instrumentlar
7. Pentest uchun kitoblar
8. Praktika uchun CTFlar
9. Pentestni boshlash
10. Kiberxavfsizlik sohasini o'rganish uchun 50 ta eng yaxshi YouTube kanallar
11. Kiberxavfsizlik kelajagi: Nega uni 2024 yilda o'rganishni boshlash kerak

1.Pentest Nima?

Pentest — tarmoq yoki dasturga xakerlik hujumiga o'xshash jarayonlarni amalga oshiruvchi test tizimi hisoblanadi. Pentestning maqsadi tizim yoki dasturni qanday himoyalanganini o'rganish. Pentest nomi "penetratsion testing" degan so'zdan olingan bo'lib, u ingliz tilidan "kirish testi" deb tarjima qilinadi

Pentest amalga oshirilayotgan jarayonda mutaxassislar tizimni buzish yoki tajovuzkorlarga maxfiy ma'lumotlarga kirish imkonini beradigan muammolarni qidiradi va tahlil qiladi. Ular shuningdek, haqiqiy tajovuzkor pozitsiyasidan turib, tizimni turli yo'llar bilan buzishga harakat qilib ko'rishadi. Shu orqali siz o'z biznes yoki kompaniyangizni kutilmagan tashqi hujumlardan asrash choralari ko'radi.

Pentestingni kim qiladi

Pentest bo'yicha mutaxassislar, yoki "oq shlyapa" xakerlari, tizimlar va tarmoqlardagi zaif tomonlarni aniqlash, hujum qanday va qayerdan amalga oshirilishi mumkinligini aniqlash, turli xakerlik hujumlarida himoyalanish qanday ishlashini aniqlash, vaziyatni yaxshilash bo'yicha tavsiyalar berish, tizimlarga haqiqiy xakerlik hujumlarining oldini olish uchun, ma'lumotlar va tarmoq salomatligi xavfsizligi va maxfiyligini ta'minlash maqsadida faoliyat yuritadi

2.Pentest qilish qanday bosqichlardan iborat?

1. **Ma’lumot to’plash:** Ochiq manbalarda, ijtimoiy tarmoqlarda, forumlarda va bloglarda tashkilot va xodimlar haqidagi ma’lumotlarni qidirish.
2. **Texnik bazani izlash:** Korxona uchun mavjud resurslar, ilovalar va texnik vositalarni aniqlash.
3. **Kamchiliklar va tahdidlarni tahlil qilish**: Pentesterlar tomonidan ishlab chiqilgan vositalar va yordamchi dasturlar to’plamidan foydalangan holda xavfsizlik tizimlari hamda ilovalardagi kamchiliklarni aniqlash.
4. **Operatsion va ma’lumotlarni qayta ishlash:** Haqiqiy kiberhujumga taqlid qilish orqali keyingi tahlil bilan har qanday zaifliklar haqida ma’lumot olish.
5. **Hisobotni yaratish**: Mavjud xavfsizlik tizimini takomillashtirish bo’yicha takliflar bilan yakunlangan pentest natijalarini loyihalash va taqdim etish

3.Pentester bo'lishni xohlaysizmi?

Agar siz "pentester" bo'lishni istasangiz, bu yo'nalishda qanday boshlash kerakligini bilmaysizmi? Men sizga bu yo'nalishda muvaffaqiyatli bo'lish uchun amaliy qadamlarni tushuntiraman. Shuningdek, ish bilan bog'liq bo'lgan ma'lumotlarni o'rganish va o'ziga xos foydalanish uchun qanday imkoniyatlarni yaratishni ko'rsataman.

1. **O'zingizni tushunish: O'zingizni tahlil qiling va pentesting sohasida ishlashga qanday qobiliyatga ega ekanligingizni aniqlang. Bu sohada ishlash uchun kerakli sifatlar va xususiyatlarga ega bo'lishingiz kerak.**
2. **Ko'nikmalarni oshirish: Kompyuter ilmi yoki axborot xavfsizligi sohasida solid ta'lim olishga e'tibor bering. Bu yo'nalishda boshlanish uchun IT sohasidagi tajribangizni oshiring. O'zgaruvchanlik va yangiliklarga tayyor bo'ling.**
3. **Xakerlik sertifikatlari: Hacking yoki penetration testing sohasida sertifikat olish juda muhimdir. CEH (Certified Ethical Hacker) yoki OSCP (Offensive Security Certified Professional) sertifikatlari bu yo'nalishda tanlangan sertifikatlardan ba'zilari.**
4. **Amaliy tajriba: Real dunyoda amaliy tajribaga ega bo'lish uchun lablar, o'quv kurslari yoki o'zlashtirilgan mashg'ulotlar bilan ishlang. TryHackMe, HackTheBox, VulnHub, Virtual Hacking Labs kabi platformalarda o'zlashtirilgan mashg'ulotlar bilan tanishib chiqing.**
5. **Ish topish: O'rgangan bilimiz bilan, vakansiyalarga rezyume junatish va kompaniyalar bilan tanishishni boshlang. LinkedIn, ish portallari va kompaniyalar veb-saytlarida ish e'lonlarini kuzating.**

4.Dasturlash tillari

Agar siz “pentester” bo’lishni istasangiz, sizga qanday dasturlash tillarini o’rganish kerakligini tushuntiraman. Bu sohada ishlash uchun bir nechta dasturlash tili mavjud, lekin quyidagi tilni o’rganishni tavsiya qilaman:

1. **Python**: Python bu sohada juda mashhur va oson til hisoblanadi. U yuqori darajada kuchli, umumiy maqsadli va ob’ektga yo’naltirilgan dasturlash tili hisoblanadi. Pythonni skript til sifatida ham, dasturlash til sifatida ham ishlatishingiz mumkin. Uning oddiy sintaksisi, ob’ektga yo’naltirilganligi, keng kutubxonalari va katta jamoa o’zgaruvchanliklarni qo’llab-quvvatlaydi. Python hacking, pen-testing va etik hacking sohalarida keng qo’llaniladi. Python orqali tarmoq vositalarini, parol qirg’inchiligi vositalarini, kalitlog’or vositalarini va GUI vositalarini oson yaratishingiz mumkin. Shuningdek, Python avtomatlashtirish vositalarini, zararli dasturlarni, exploit yozishni va boshqalarini yaratishda ham foydalaniladi. Python kross-platformani qo’llab-quvvatlaydi, ya’ni bir vaqtda bir nechta platformalarda ishga tushirilishi mumkin.
2. **Java**: Java boshqa mashhur dasturlash tili hisoblanadi. Python bilan o’xshash, Java ham keng qo’llaniladigan dasturlash tili. Lekin, Python kabi skript til sifatida ishlatilmaydi. Java ochiq manbali, kross-platformali, kuchli va umumiy maqsadli dasturlash tili hisoblanadi. Java web dasturlash, ilovalar dasturlash, xizmatlarni yaratish va boshqa ko’plab sohalarda ishlatiladi. Java ham hacking va pen-testing sohalarida foydalaniladi.
3. **C#:** C# dasturlash tili ham pentesterlar tomonidan keng qo’llaniladi. Bu til orqali kriptor, binder, dropper, RAT, ransomware, fuzzing va boshqa qo’llanmalar yaratish mumkin. Shuningdek, ushbu til xavfsizlik vositalarini avtomatlashtirishda ham ishlatiladi

5. Kontent menedjerlar (CMS)

Jahon bo'ylab eng ko'p ishlatiladigan 10 CMS

1. WordPress: WordPress dunyoning eng mashhur CMS tizimi hisoblanadi. U oson, kuchli va keng qo'llaniladigan tizimdir. WordPress orqali bloglar, korporativ veb-saytlar, onlayn do'konlar va boshqa turlardagi saytlarni yaratish mumkin
2. Shopify: Shopify onlayn do'konlar uchun maxsus CMS tizimi. U mahsulotlar sotish, inventar, to'lovlar va boshqa e-commerce funktsiyalarini o'z ichiga oladi. Shopify orqali osonlik bilan onlayn do'kon yaratishingiz mumkin
3. Wix: Wix oson va intuitiv CMS tizimi. U drag-and-drop interfeysi orqali veb-saytlarni yaratishga imkon beradi. Wix orqali shaxsiy bloglar, portfellar va korporativ saytlarni yaratishingiz mumkin
4. Joomla!: Joomla! kuchli va keng qo'llaniladigan CMS tizimi. U korporativ saytlar, forumlar, bloglar va boshqa turlardagi saytlarni yaratishda foydalaniladi. Joomla! o'zgaruvchan va keng imkoniyatlarga ega.
5. Drupal: Drupal katta tashkilotlar va korporativ saytlar uchun mo'ljallangan CMS tizimi. U xavfsizlik va tarmoqni boshqarishga katta e'tibor beradi. Drupal orqali keng qo'llaniladigan saytlar yaratishingiz mumkin.
6. Blogger: Blogger Google tomonidan taqdim etilgan oson va bepul CMS tizimi. U blog yaratishga imkon beradi va Google Blogger orqali hosting va domenni taqdim etadi.
7. Magento: Magento e-commerce saytlari uchun mo'ljallangan CMS tizimi. U mahsulotlar sotish, inventar, to'lovlar va boshqa e-commerce funktsiyalarini o'z ichiga oladi. Magento kuchli va o'zgaruvchanliklarga ega.
8. Squarespace: Squarespace oson va dizaynli CMS tizimi. U portfellar, bloglar va korporativ saytlar uchun mo'ljallangan. Squarespace orqali osonlik bilan saytlarni yaratishingiz mumkin.
9. PrestaShop: PrestaShop e-commerce saytlari uchun mo'ljallangan CMS tizimi. U mahsulotlar sotish, inventar, to'lovlar va boshqa e-commerce funktsiyalarini o'z ichiga oladi. PrestaShop o'zgaruvchan va keng imkoniyatlarga ega.

10. Ghost: Ghost blog yaratish uchun mo'ljallangan CMS tizimi. U oson va fokuslangan blog yaratishga imkon beradi. Ghost orqali osonlik bilan blog yaratishingiz mumkin.

Agar siz "pentester" bo'lishni istasangiz, CMS (Content Management System) tizimlarini tekshirishda qanday vositalardan foydalanishingiz kerakligini tushuntiraman. CMS tizimlari veb-saytlarni boshqarish uchun ishlatiladi va ularga xususiy modullar, plaginlar, komponentlar va mavjud dizaynlar (themes) bo'lishi mumkin. Bu tizimlar o'zlariga xos xavfsizlik muammolari va kuchli nuqtalari bor.

Quyidagi CMS tizimlarini tekshirishda foydalanishingiz mumkin:

1. cms-explorer: Bu vosita CMS veb-saytlarida ishlatiladigan modullar, plaginlar, komponentlar va dizaynlar haqida ma'lumot beradi. Shuningdek, ularga bog'liq xavfsizlik muammolari haqida ma'lumotlar ham mavjud.
2. DET (Data Exfiltration Tool): DET CMS tizimlarida DLP (Data Loss Prevention) sozlamalaridagi xato va muammolarni aniqlash uchun ishlatiladi. Bu vosita CMS tizimlaridan ma'lumotlarni olib chiqish imkoniyatiga ega.
3. EyeWitness: Bu vosita CMS veb-saytlarini skrinshot olish, server sarlavhasini va standart kirish ma'lumotlarini tekshirish uchun ishlatiladi.
4. WPScan: Bu vosita orqali agar sayt Wordpressda ishlasha audit o'tqaza olasiz va zaif tomonlarini aniqlaysiz.

6. Instrumentlar

Kategoriya bo'yicha instrumentlar

Informatsiya yig'ish uchun:

Instrument	Dastrulash Tili	OS	Vazifasi
Harvester	Python	Linux/Windows/macOS	Elektron pochta, subdomenlar va nomlar Harvester.
CTFR	Python	Linux/Windows/macOS	HTTPS veb-saytlari subdomenlarini olish uchun sertifikat shaffofligi jurnallarini suiiste'mol qilish.
Sn1per	bash	Linux/macOS	Avtomatlashtirilgan Pentest Recon Scanner.
QIZIL kalxat	PHP	Linux/Windows/macOS	Ma'lumot to'plash, zaifliklarni skanerlash va skanerlash uchun barchasi bitta vositada. Barcha penetratsion sinovchilar uchun bo'lishi kerak bo'lgan vosita.
Infoga	Python	Linux/Windows/macOS	Elektron pochta ma'lumotlarini yig'ish.
KnockMail	Python	Linux/Windows/macOS	Elektron pochta manzili mavjudligini tekshiring.
a2sv	Python	Linux/Windows/macOS	SSL zaifligiga avtomatik skanerlash.
Wfuzz	Python	Linux/Windows/macOS	Veb-ilova fuzzer.
Nmap	C/C++	Linux/Windows/macOS	Juda keng tarqalgan vosita. Tarmoq xosti, vuln va port detektori.
PhoneInfoga	Bor	Linux/macOS	Telefon raqamlari uchun OSINT ramkasi.

Parolni buzish uchun:

Instrument	Dastrulash Tili	OS	Vazifasi
Jon Ripper	C	Linux/Windows/macOS	Jon Ripper - bu tezkor parolni buzuvchi.
hashcat	C	Linux/Windows/macOS	Dunyodagi eng tez va ilg'or parolni tiklash yordam dasturi.
Gidra	C	Linux/Windows/macOS	Hujum qilish uchun ko'plab protokollarni qo'llab-quvvatlaydigan parallel kirish krakeri.
ophcrack	C++	Linux/Windows/macOS	Kamalak jadvallari asosidagi Windows parolini buzuvchi.
Ncrack	C	Linux/Windows/macOS	Yuqori tezlikdagi tarmoq autentifikatsiyasini buzish vositasi.
WGen	Python	Linux/Windows/macOS	Python yordamida ajoyib so'zlar ro'yxatini yarating.
SSH auditori	Bor	Linux/macOS	Tarmoqdagi zaif ssh parollarini skanerlashning eng yaxshi usuli.

WiFi'ni test qilish uchun:

Instrument	Dastrulash Tili	OS	Vazifasi
Aircrack	C	Linux/Windows/mac OS	WiFi xavfsizligini tekshirish vositalari to'plami.
bettercap	Go	Linux/Windows/mac OS/Android	bettercap - tarmoq hujumlari va monitoringi uchun Shveytsariya armiyasi pichog'i.
WiFi Pumpkin	Python	Linux/Windows/mac OS/Android	Rogue Wi-Fi kirish nuqtasi hujumi uchun ramka.
Airgeddon	Shell	Linux/Windows/mac OS	Bu simsiz tarmoqlarni tekshirish uchun Linux tizimlari uchun ko'p ishlatiladigan bash skriptidir.
Airbash			POSIX-mos keluvchi, to'liq avtomatlashtirilgan WPA PSK qo'l siqish skripti penetratsiya sinoviga qaratilgan.

Ekspluatatsiya uchun:

Instrument	Dastrulash Tili	OS	Vazifasi
SQLmap	Python	Linux/Windows/mac OS	Avtomatik SQL in'ektsiyasi va ma'lumotlar bazasini egallash vositasi.
XSStrike	Python	Linux/Windows/mac OS	Kengaytirilgan XSS aniqlash va ekspluatatsiya to'plami.
Commix	Python	Linux/Windows/mac OS	Avtomatlashtirilgan All-in-One OT buyruqlarini kiritish va ekspluatatsiya qilish vositasi.

Web saystni tekshirish uchun:

Instrument	Dastrulash Tili	OS	Vazifasi
Nuclei	Go	Linux/Windows/macOS	Oddiy YAML asosidagi DSL-ga asoslangan tez va sozlanishi zaiflik skaneri.
WPScan	Ruby	Linux/Windows/macOS	WPScan - qora quti WordPress zaiflik skaneri.
Droopescan	Python	Linux/Windows/macOS	Bir nechta CMS, asosan Drupal va Silverstripe bilan bog'liq muammolarni aniqlash uchun plaginga asoslangan skaner.
Joomscan	Perl	Linux/Windows/macOS	Joomla zaiflik skaneri.
Drupwn	Python	Linux/Windows/macOS	Drupal xavfsizlik skaneri Drupal-ga asoslangan veb-ilovalarda sanab o'tish uchun.
CMSeek	Python	Linux/Windows/macOS	CMS aniqlash va ekspluatatsiya to'plami - WordPress, Joomla, Drupal va boshqa 130 CMS-ni skanerlang.
Burp Suite	Java	Linux/Windows/Mac OS	Web saytlarni xavfsizligini tekshirish uchun eng ko’p ishlatiladigan instrument

7. Pentest uchun kitoblar

1. The hacker playbook
2. The hacked playbook 2
3. The hacked playbook 3
4. Linux Basics
5. Learn Linux quickly
6. Penetration Testing: A Hands-On Introduction to Hacking
7. Kali Linux Revealed - PDF (2017)
8. Blue Team Field Manual (BTFM) (2017)
9. Cybersecurity - Attack and Defense Strategies (2018)
10. NMAP Network Scanning : Official Discovery (2009)
11. Social Engineering : The Art of Human Hacking (2010)
12. Incognito Toolkit: Tools, Apps, and Creative Methods for Remaining Anonymous

8. Praktika uchun CTFlar

№		
1	Vulnhub	O'ynash uchun juda ko'p VMlar mavjud. Ba'zilar yangi boshlanuvchilar uchun mos, ba'zilari esa yo'q.
2	Itsecgames	bWAPP yoki buggy veb-ilovasi ataylab xavfsiz bo'lmagan veb-ilovadir.
3	Dvwa	La'nati zaif veb-ilova - bu o'z mahoratingizni mashq qilish uchun ataylab xavfsiz bo'lmagan yana bir veb-ilova.
4	Hackthissite	Xakerlik mahoratingizni oshirish uchun qiyinchiliklar, CTF va boshqalarni taqdim etadigan sayt.
5	Defend the Web	Defend the Web - bu o'z mahoratingizni o'rganishingiz va sinab ko'rishingiz mumkin bo'lgan interaktiv xavfsizlik platformasi.
6	Root-me	Sizning xakerlik qobiliyatingizni sinab ko'rish uchun qiyinchiliklarga mezbonlik qiladigan yana bir veb-sayt.
7	HackTheBox	Penetratsiya testlari va kiberxavfsizlik bo'yicha ko'nikmalaringizni sinab ko'rish va oshirish uchun onlayn platforma.
8	Overthewire	Qiziqarli o'yinlar shaklida xavfsizlik tushunchalarini o'rganing va mashq qiling.
9	Ctftime	CTF bilan bog'liq barcha narsalar uchun de-fakto veb-sayt.
10	TryHackMe	TryHackMe - bu amaliy mashqlar va laboratoriyalardan foydalangan holda kiberxavfsizlikni o'rganish uchun bepul onlayn platforma.
11	PicoCTF	Sizga mashq qilish uchun turli darajadagi qiyinchilikdagi qiziqarli CTF topshiriqlarini taqdim etadi.

9. Pentestni boshlash

1. Kali Linux o’rnating, barcha instrumentlari bilan tanishib chiqing. Kali Linuxni saytida barcha ma’lumotlar bor.
2. Ingliz tilini har kuni o’rganing
3. Youtube kali linux haqida videodarslarni ko’rib chiqing
4. Doim google’dan so’rang. Google bilmaydigan savol yo’q. Sizgacha doim kimdir bergan va kimdir javob yozib qoldirgan.

10.Kiberxavfsizlik sohasini o'rganish uchun 50 ta eng yaxshi YouTube kanallar:

1. NetworkChuck
2. HackerSploit
3. The Cyber Mentor
4. Null Byte
5. Computerphile
6. Cyb3rC0nci3rg3
7. Cyber Security and IT Career Information
8. David Bombal
9. Professor Messer
10. Hak5
11. LiveOverflow
12. Tech With Tim
13. NahamSec
14. SecurityFWD
15. IPGraySpace
16. Chris Titus Tech
17. Elevator
18. Jon Good
19. StationX
20. Stok

21. Security Weekly
22. Infosec Institute
23. MalwareTech
24. Gynvael Coldwind
25. John Hammond
26. OpenSecurityTraining
27. SecureNinjaTV
28. SANS Cyber Aces
29. CISO Series
30. CyberXplained
31. SecuraBit
32. TechChip
33. Engineer Man
34. SecuriDex
35. Cyberspatial
36. Michael Bazzell
37. The PC Security Channel
38. Black Hills Information Security
39. IppSec

40. Cyber Insecurity
41. Zimperium
42. Pentester Academy TV
43. Practical Ethical Hacking
44. The Modern CISO
45. Hacker101
46. Deviant Ollam
47. Cyber Arsenal
48. Darknet Diaries
49. Bugcrowd
50. The Cybersecurity Analyst

11. Kiberxavfsizlik kelajagi: Nega uni 2024 yilda o’rganishni boshlash kerak

1️⃣ Kiberxavfsizlik bo'yicha mutaxassislarga talab yuqori va sun'iy intellekt ishingizni ololmaydi

2️⃣ Kiberxavfsizlik ko'plab sohalarda qo'llash mumkin. Bu degani qishloqdaham ish topasiz

3️⃣ Kiberxavfsizlikda qolgan IT sohalardan ko'p daromad topish mumkin

4️⃣ Kiberxavfsizliksiz biznes bu 7kunlik ish joyi xodimlar uchun.

5️⃣ Kiberxavfsizlik - Nomi ulug' daromadi undanda ulug'

6️⃣ Kiberxavfsizlik - bu har kuni o'qish o'rganish kerak degani.

7️⃣ Kiberxavfsizlik yaqinlarizni kibertahdidlardan himoyalanish uchun zarur.

8️⃣ Kiberxavfsizlik bu hammasi degani, kod yozish, psixologiya, dokumentatsiya, kitob yozish

9️⃣ Kiberxavfsizlik kartangizdagi pulini o'g'irlanishining oldini olishga yordam beradi

0️⃣ Kiberxavfsizlik shaxsiy xavfsizlik va maxfiylikni oshira keyin VPN va Tor emas balki VPS ishlatasiz