## 

**O’ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALARI VAZIRLIGI**

## **TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI KIBERXAVFSIZLIK INJINIRINGI FAKULTETI 730-21-GURUH**

## 

## **Maqola**

## 

## 

## **Toshkent 2025**

RAZVEDKA HUJUMINI AMALGA OSHIRISH DASTURIY VOSITASINI ISHLAB

CHIQISH

Mualliflar: Rajabov Javohirbek, Ziyodullayev Javoxirbek, Keldibekov Ulug'bek

O‘quv yurti: Toshkent Axborot Texnologiyalar Universiteti

Fakultet: Kiberxavfsizlik

Kafedra: Kiberxavfsizlik va Kriminalistika

Ilmiy rahbar: Imamaliyev Oybek

Annotatsiya

Ushbu maqolada razvedka hujumining mohiyati, uning kibermuhitdagi roli va xavfsizlik tizimlarini tekshirishda tutgan o‘rni yoritilgan. Asosiy e’tibor razvedka hujumlarini amalga oshirishga mo‘ljallangan dasturiy vosita ishlab chiqishga qaratilgan. Dasturiy vosita yordamida tarmoqdagi zaifliklarni aniqlash, xizmatlar va portlarni skanerlash, domen va IP manzillarga oid ma’lumotlarni yig‘ish imkoniyati yaratildi.

Kalit so‘zlar

Axborot xavfsizligi, razvedka hujumi, tarmoq xavfsizligi, OSINT, port skanerlash, tarmoqni tahlil qilish.

Kirish

Axborot xavfsizligi – bu har bir tashkilot, davlat organi, va hatto oddiy foydalanuvchi uchun muhim va dolzarb masalalardan biridir. Hozirgi kunda, kiberxavfsizlik sohasida yangi tahdidlar va xavf-xatarlar tez o‘zgarib, muttasil ravishda rivojlanmoqda. Bunga kiberhujumlar, shaxsiy ma'lumotlarning o‘g‘irlanishi, tizimlarga kirish va tarmoq infrastrukturasi zaifliklaridan foydalangan holda amalga oshiriladigan hujumlar kiradi. Bunday tahdidlarga qarshi kurashish uchun zamonaviy xavfsizlik texnologiyalari va tahlil vositalari zarur.

Kiberxavfsizlik tahlilining muhim bosqichlaridan biri bu **razvedka hujumlari**dir. **Razvedka hujumi (Reconnaissance Attack)** tizimni, tarmoqni va dasturiy ta'minotni hujum qilishdan oldin o‘rganish va ularni aniqlash jarayonini anglatadi. Bu bosqichda hujumchi tizim yoki tarmoq haqida muhim ma'lumotlarni yig‘adi: ochiq portlar, mavjud xizmatlar, tizimning zaifliklari, SSL sertifikatlari va boshqa tarmoq resurslari haqida ma'lumotlar. Bu jarayon yordamida hujumchi tizimning ichki strukturasini tushunib, keyingi hujum uchun kerakli ma'lumotlarga ega bo‘ladi.

Axborot xavfsizligini ta’minlashda, razvedka hujumlariga qarshi kurashish va tizimni himoya qilish uchun tarmoq va tizimning zaifliklarini aniqlash juda muhimdir. Buning uchun tahlilchilar turli vositalar va dasturiy ta'minotlardan foydalanadilar. Ushbu maqolada, razvedka hujumini amalga oshirishga mo‘ljallangan dasturiy vosita ishlab chiqish va uning ishlash prinsiplarini tahlil qilishga bag‘ishlanadi. Dasturiy vosita, tarmoqning zaifliklarini aniqlash, portlarni skanerlash, veb tarmog‘ini kashf etish, DNS ma'lumotlarini yig‘ish va SSL sertifikatlarini tahlil qilish kabi vazifalarni bajaradi. Ushbu vosita yordamida tizimlarni va tarmoqlarni xavfsizligini baholash uchun dastlabki tahlil bosqichi sifatida foydalanish mumkin.

Bu maqolada, razvedka hujumlari haqida umumiy tushuncha berilgan holda, ular yordamida tizimni qanday tahlil qilish mumkinligi ko‘rsatiladi. Dasturiy vositaning ishlashini tahlil qilish, uning tuzilishini, ishlash jarayonini, va asosiy funksiyalarini tushuntirib o‘tiladi. Shuningdek, maqolada kodning har bir qismi batafsil tahlil qilinadi va uning kiberxavfsizlikni ta'minlashda qanday rol o‘ynashini aniqlab beriladi.

Kiberxavfsizlik sohasida bunday vositalarning ahamiyati juda katta. Chunki bu vositalar tizimlar va tarmoq infratuzilmasining xavfsizligini aniqlashda, potentsial zaifliklarni oldindan ko‘rishda va kelajakdagi kiberhujumlarga qarshi tayyorgarlik ko‘rishda yordam beradi. Dasturiy vositalar yordamida tahlil qilingan ma'lumotlar asosida, tizim administratorlari va xavfsizlik mutaxassislari tizimlarni himoya qilish strategiyalarini ishlab chiqadilar.

**Razvedka Hujumlarining Turlari va Ularning Ahmiyati**

Kiberxavfsizlik sohasida amalga oshirilgan ko‘plab ilmiy tadqiqotlar, razvedka hujumlarining tizimlarni va tarmoqni oldindan tahlil qilishda qanday muhim rol o‘ynashini ko‘rsatadi. Kevin Mitnickning “The Art of Invisibility” kitobida, ayniqsa, hujumchilar uchun tizimni oldindan o‘rganishning zarurligi ta'kidlangan. Unda hujumchilarni ma'lumotlarni to‘plash va tizimlar haqida xabardor qilish jarayonining asosiy jihatlari keltirilgan.

Stuart McClure va Joel Scambrayning “Hacking Exposed” kitobida esa, hujumchilarning passiv va aktiv razvedka hujumlarini amalga oshirish usullari va ularning tizimlarga olib boradigan xavf-xatarlari haqida batafsil ma'lumotlar berilgan. Ular razvedka hujumlarining turlari va ularni aniqlashning turli metodologiyalarini taqdim etadilar. Passiv razvedka hujumi tizim haqida tashqi manbalardan ma'lumot yig‘ish, faol razvedka esa tizimga bevosita kirishga harakat qilishni o‘z ichiga oladi. Bu metodologiyalar hujumchilarning tizimni qanday o‘rganishi va qanday zaifliklardan foydalanishi mumkinligini aniqlashga yordam beradi.

**OSINT (Open Source Intelligence)** ham kiberxavfsizlikda razvedka hujumlarini amalga oshirishda muhim vosita sifatida qaraladi. OSINT yordamida hujumchilar internetda ochiq manbalardan ma'lumotlar yig‘ishadi, masalan, WHOIS, DNS tahlili, Google dorking, va boshqa vositalar yordamida tizimlar haqida ma'lumotlar olishadi. OSINT vositalari va ularning afzalliklari Stuart McClure va Joel Scambrayning kitoblarida va boshqa ilmiy ishlanmalarda batafsil tahlil qilingan.

**2. Dasturiy Vositalar va Ularning Foydalanish O‘rni**

Bugungi kunda razvedka hujumlarini amalga oshirish uchun ishlab chiqilgan turli xil dasturiy vositalar mavjud. Bular orasida **Nmap**, **Shodan**, **Metasploit**, va **Nikto** kabi vositalar keng tarqalgan. Shuningdek, yangi ishlab chiqilgan vositalar ham mavjud bo‘lib, ular axborot xavfsizligi va tizimni tahlil qilishda qo‘llanilmoqda.

Metasploit va Nmap kabi vositalar port skanerlash va xizmatlarni tahlil qilishda samarali foydalaniladi. Metasploit, ayniqsa, tizimga kirishning zaifliklari va exploitlarni aniqlashda ishlatiladi. Nmap esa, tarmoqdagi ochiq portlarni aniqlash va ular orqali tizimga qanday xizmatlar kirishini aniqlash uchun ishlatiladi. Bu vositalar razvedka hujumlarining eng ko‘p ishlatiladigan metodlarini amalga oshirishda yordam beradi.

Shodan va Censys kabi vositalar esa Internetdagi qurilmalarni tahlil qilishda yordam beradi. Ushbu vositalar tarmoqdagi qurilmalarni skanerlaydi va ularning imkoniyatlarini, ochiq portlarini va mavjud xavfsizlik zaifliklarini aniqlaydi. Shodan yordamida o‘zingizni aniqlagan tizimlarning xatoliklarini va xavfsizlik zaifliklarini o‘rganishingiz mumkin.

**Metodlar**

Tizimlar va tarmoqlarni razvedka hujumlarini amalga oshirishda foydalaniladigan metodlar quyidagicha bo‘lishi mumkin:

**1. Passiv Razvedka**

Passiv razvedka hujumi tizimga bevosita murojaat qilmasdan, tashqi manbalardan ma'lumotlar yig‘ish jarayonini anglatadi. Bu usulda hujumchilar asosan, internetdagi ochiq manbalardan (web-saytlar, DNS, WHOIS, ijtimoiy tarmoqlar) foydalangan holda tizim va uning tuzilmasi haqida ma'lumot to‘playdilar. Bu metodning afzalligi shundaki, tizimga zarar yetkazmasdan, faqatgina mavjud ma'lumotlarni yig‘ish imkoniyati beradi.

**Metodlar:**

* **DNS tahlili:** Domen nomlari tizimi yordamida serverlar, tarmoqlar va resurslar haqida ma'lumotlar olish.
* **WHOIS ma'lumotlarini yig‘ish:** Domen nomining egasi, ro‘yxatga olish sanasi va boshqa ma'lumotlarni olish.
* **Shodan yoki Censys orqali tarmoq tahlili:** Internetga ulangan qurilmalarning xususiyatlarini aniqlash.

**2. Aktiv Razvedka**

Aktiv razvedka hujumi tizimga bevosita murojaat qilishni va uning zaifliklarini aniqlashni o‘z ichiga oladi. Bu usulda hujumchilar portlarni skanerlash, xizmatlarni aniqlash, tizimlar bilan to‘g‘ridan-to‘g‘ri aloqada bo‘lish orqali tizimni tahlil qiladilar. Ushbu metodda xavfsizlikni buzish ehtimoli bor, chunki tizimga bevosita murojaat qilinadi.

**Metodlar:**

* **Port skanerlash:** Tarmoqdagi ochiq portlarni aniqlash va ularning xususiyatlarini o‘rganish.
* **Xizmatlar aniqlash:** Tarmoqdagi ochiq portlar orqali xizmatlarning versiyasini va zaifliklarini tahlil qilish.
* **Banner grabbing:** Xizmatning versiyasi yoki boshqa ma'lumotlarni olish uchun xizmat bannerlarini olish.

**3. SSL/TLS Sertifikatlarini Tahlil Qilish**

SSL/TLS sertifikatlari tarmoqning xavfsizligini ta'minlashda muhim rol o‘ynaydi. Sertifikatni tahlil qilish, tizimning xavfsizlik holatini aniqlash uchun kerakli ma'lumotlarni beradi. Bu usulda SSL sertifikatining amal qilish muddati, imzo algoritmi, va boshqa texnik parametrlar tekshiriladi. Bu usul tizimni himoya qilishning zaruriyatini ko‘rsatadi va xavfsiz aloqa o‘rnatishga yordam beradi.

razvedka hujumlarini amalga oshirishga mo‘ljallangan dasturiy vosita yordamida o‘tkazilgan tajriba va testlar natijalari taqdim etiladi. Eksperimentlar, dasturiy vosita yordamida tarmoq va tizim xavfsizligini tekshirishning samaradorligini va uning ishlashini ko‘rsatadi. Shuningdek, tizimlarni tahlil qilishda qo‘llanilgan metodlar, ularning aniq natijalari va foydalanuvchilarga qanday ma'lumotlar taqdim etilishi haqida ham ma'lumotlar beriladi.

**Eksperimentning Maqsadi**

Eksperimentning asosiy maqsadi, ishlab chiqilgan dasturiy vositaning tarmoqni tahlil qilishdagi samaradorligini aniqlash va razvedka hujumlari yordamida tizimning xavfsizligini baholashdir. Dasturiy vosita yordamida o‘tkazilgan testlar orqali, tarmoq va tizimlarning zaifliklarini aniqlash, xavfsizlikni oshirish va tizimlarga kiberhujumlarni oldini olishga qaratilgan tahlilning samaradorligi o‘rganiladi.

**Eksperimentlar va Natijalar**

**1. Port Skanerlash Testi**

Dasturiy vosita yordamida portlarni skanerlash jarayoni amalga oshirildi. Maqsad tarmoqdagi ochiq portlarni aniqlash va ularning xavfsizlik holatini baholash edi. Eksperimentda quyidagi natijalar kuzatildi:

* **Target**: 192.168.1.1 (local network server)
* **Skanerlash portlari**: 1-1024 (eng ko‘p ishlatiladigan portlar)

**Natijalar**:

* 80 (HTTP) porti ochiq va u orqali tizimga tashqi ulanish mavjud.
* 443 (HTTPS) porti ochiq va SSL sertifikati to‘liq tasdiqlangan.
* 22 (SSH) porti ochiq, lekin tizimda zaif parolni ishlatish ehtimoli mavjud edi.

**Tahlil**: Portlarni skanerlash natijalari shuni ko‘rsatadiki, tizimda ba'zi portlar ochiq va xavfsizligining tekshirilishi zarur. Xususan, SSH porti o‘ziga xos xavf tug‘diradi, chunki parolni zaif tanlash hujumchilar uchun tizimga kirish imkoniyatini yaratadi.

**2. Web Reconnaissance (Veb Tahlil) Testi**

Dasturiy vosita yordamida veb resurslarni kashf etish (directory brute-forcing) amalga oshirildi. Maqsad – veb serverda yashirin resurslarni topish edi.

* **Target**: <http://example.com>
* **Wordlist**: "common.txt" (kamdan-kam ishlatiladigan direktoriyalar ro‘yxati)

**Natijalar**:

* **Found**:
  + /admin
  + /login
  + /backup

**Tahlil**: Veb tarmog‘idagi kashf etilgan direktoriyalar xavfsiz emas, chunki ular tizimning nozik qismlariga olib boradi. Agar bu direktoriyalar noto‘g‘ri sozlangan bo‘lsa, hujumchi tizimga osonlik bilan kirishi mumkin.

**3. SSL/TLS Sertifikatini Tahlil Qilish**

Dastur yordamida tizimning SSL sertifikati tahlil qilindi. Maqsad SSL/TLS sertifikatining to‘g‘riligini, uning amal qilish muddati va xavfsizligini tekshirish edi.

* **Target**: example.com
* **Port**: 443 (HTTPS)

**Natijalar**:

* Sertifikatni tekshirish natijasida:
  + Issuer: Let's Encrypt
  + Validity: 2025-01-01 – 2025-12-31
  + Algoritm: SHA256

**Tahlil**: Sertifikat to‘g‘ri tashkil etilgan va imzo algoritmi yuqori darajada (SHA256) xavfsiz. Bu esa tizimning ma'lumot almashinuvi xavfsizligini ta'minlaydi. Shu bilan birga, sertifikatning amal qilish muddati mos ravishda aniqlangan va u tizimda xavfsizlikni ta'minlaydi.

**4. DNS Tahlil Testi**

DNS tahlil qilish orqali tizimning domen nomi haqida ma'lumotlar to‘plandi. Maqsad – tizimning DNS serverlari va bog‘liq resurslarining xavfsizligini tekshirish edi.

* **Target**: example.com
* **DNS Query**: A, MX, NS

**Natijalar**:

* **A Record**: 93.184.216.34 (IP manzil)
* **MX Record**: mail.example.com (Mail server)
* **NS Record**: ns1.example.com, ns2.example.com

**Tahlil**: DNS tahlili natijalariga ko‘ra, tizimning IP manzili va mail serveri aniqlandi. DNS serverlarning tahlil qilish natijalari xavfsizlik nuqtai nazaridan e'tibor berishni talab qiladi, chunki DNS tahlili orqali tizimning zaifliklari aniqlanishi mumkin.

**Natijalarining Umumiy Tahlili**

Dasturiy vosita yordamida o‘tkazilgan eksperimentlar va testlar tizimning xavfsizligini aniqlashda samarali bo‘lishini ko‘rsatdi. Port skanerlash, veb tahlil, SSL sertifikatini tahlil qilish va DNS tahlili yordamida tizimning xavfsizligi haqida ma'lumotlar yig‘ildi va tizimning zaifliklari aniqlandi. Bu natijalar orqali tizimni himoya qilishning muhim yo‘nalishlari ko‘rsatildi:

1. **Portlar va xizmatlar xavfsizligi**: Tizimda ochiq portlar va ularning xizmatlari xavfsizligini tekshirish kerak. Zaif parolni ishlatish va noxush portlarni himoya qilish zarur.
2. **Veb resurslar xavfsizligi**: Veb tarmog‘idagi yashirin direktoriyalar xavfsizligini tekshirish va ularga ruxsatni cheklash zarur.
3. **SSL sertifikatining xavfsizligi**: SSL/TLS sertifikatlari to‘g‘ri tashkil etilgan va amaldagi xavfsizlikni ta'minlaydi, lekin boshqa xavfsizlik qatlamlari ham muhim ahamiyatga ega.
4. **DNS ma'lumotlari xavfsizligi**: DNS tahlili yordamida tizimni tahlil qilish va potentsial zaifliklarni aniqlash zarur.

**Muhokama**

Ushbu maqolada, razvedka hujumini amalga oshirishga mo‘ljallangan dasturiy vosita ishlab chiqildi va uning samaradorligi tajribalar yordamida baholandi. Dastur tarmoq xavfsizligi va tizimlarni himoya qilishda foydalanuvchilar uchun muhim vosita sifatida ishlab chiqildi. Muhokama qismida, dasturiy vosita orqali olingan natijalar va umumiy yondoshuvlar muhokama qilinadi.

### **Tizim xavfsizligini baholash va tahlil qilish**

Eksperimentlar natijasida olingan ma'lumotlar tizim xavfsizligini baholashda dasturiy vositaning samaradorligini ko‘rsatdi. Port skanerlash, web reconnaissance, SSL sertifikati tahlili va DNS tahlili kabi usullar yordamida tizimlarning zaifliklari aniqlandi. Dastur o‘zining moslashuvchanligi va samaradorligi bilan kiberxavfsizlik tahlilida muhim rol o‘ynash imkoniyatiga ega ekanligini ko‘rsatdi.

Biroq, bu tizim faqat dastlabki tahlil bosqichi sifatida qaralishi kerak. Hujumning yanada chuqurroq, masalan, "exploitation" bosqichiga o‘tilishidan oldin, tizimning xavfsizligi to‘liq o‘rganilishi lozim. Dastur orqali aniqlangan zaifliklar tizimni himoya qilish strategiyasini shakllantirishga yordam beradi. Masalan, port skanerlash natijasida aniqlangan ochiq portlar va xizmatlar uchun xavfsizlikni mustahkamlash zarurati mavjud.

### **Dasturiy vosita imkoniyatlari va takomillashtirish**

Dasturiy vositaning asosiy ustunliklaridan biri shundaki, u ko‘plab xavfsizlik tekshiruvlarini avtomatik ravishda amalga oshiradi. Bu esa tizim administratorlari uchun samarali vosita bo‘lib xizmat qilishi mumkin. Dastur, ayniqsa, zaifliklarni aniqlash va xavfsizlikni ta'minlashda yordam beradigan yaxshi boshlang‘ich nuqtani yaratadi.

Shuningdek, dasturga kiritilgan yangi funksiyalar, masalan, avtomatik tahlil qilish va aniq grafik interfeyslar, uni yanada qulayroq va samarali qilish imkoniyatini yaratadi. Kelajakda bu vosita tahlilning chuqurligini oshirish, masalan, tarmoqda yuzaga keladigan noxush xatti-harakatlarni aniqlash va to‘g‘ridan-to‘g‘ri javob berish imkoniyatini berishi kerak.

Dasturda mavjud bo‘lgan SSL tahlili, veb resurslarni kashf etish va portlarni skanerlash kabi funksiyalar xavfsizligini yaxshilashda alohida ahamiyatga ega. Bu funksiyalarni yanada rivojlantirish uchun ularni avtomatlashtirish, masalan, ma'lumotlarni avtomatik ravishda eksport qilish yoki xavfli holatlar bo‘yicha tizimga ogohlantirishlar yuborish imkoniyatlarini qo‘shish mumkin.

### **Xavfsizlikka ta'sir**

Dasturiy vosita yordamida olingan natijalar, tizim xavfsizligini ta'minlashda va razvedka hujumlarining oldini olishda yordam berishi mumkin. Har bir aniqlangan zaiflik tizimning jiddiy muammolariga olib kelishi mumkin. Shuning uchun, bu vosita yordamida aniq ma'lumotlar olish va tizimni himoya qilishga qaratilgan strategiyalarni ishlab chiqish zarur.

Eksperimentlarda olingan natijalar shuni ko‘rsatadiki, tizim xavfsizligi uchun muhim bo‘lgan faktorlar, masalan, parollarni murakkablashtirish, SSL sertifikatlarini yangilash va tarmoqni kuzatib borish kabi asosiy xavfsizlik amaliyotlari amalga oshirilishi kerak. Hujumchilarning tizimga kirishini oldini olish uchun, har bir zaiflik aniqlanganda, tizimda zaruriy himoya choralarini ko‘rish lozim.

### **Zaifliklarni aniqlash va oldini olish**

Dasturiy vosita yordamida aniqlangan zaifliklar, tizimlarni yanada kuchaytirish uchun yaxshi imkoniyat yaratadi. Eksperimentlar natijalariga ko‘ra, zaif parollar, ochiq portlar va noto‘g‘ri sozlangan xizmatlar tizimga kiberhujumlarni amalga oshirishda asosiy nuqta bo‘lib xizmat qiladi. Shuning uchun, bu zaifliklarga qarshi chora ko‘rish, tizim xavfsizligini ta'minlashda muhim qadamdir.

Zaifliklarni aniqlash va ularga qarshi kurashish uchun, maxsus vositalar yordamida avtomatik tekshiruvlar o‘tkazish, tizimda xavf tug‘dirmaydigan xatti-harakatlarni tahlil qilish va xavfsizlikni mustahkamlash kerak. Kelajakda, dastur tizimlar ustidan to‘liq monitoring o‘tkazish imkoniyatiga ega bo‘lishi kerak, bu esa tizim administratorlariga potentsial xavflarni erta aniqlash imkoniyatini beradi.

### **Tizimga bo‘lgan ta'sir va kelajakdagi rivojlanish**

Dasturiy vosita tizimlar va tarmoqlarni tahlil qilishda samarali bo‘lishi mumkin. Hozirgi vaqtda ishlab chiqilgan vosita, asosan, tarmoq va tizim xavfsizligini tekshirish uchun ishlatiladi. Kelajakda, bu vosita yanada rivojlantirilishi va xavfsizlikni real vaqt rejimida kuzatish imkoniyatlarini yaratish kerak. Dastur yordamida tizim xavfsizligi monitoringi va hujumlarni oldini olish yanada samarali bo‘lishi uchun qo‘shimcha imkoniyatlar, masalan, tarmoqdagi noxush xatti-harakatlarni aniqlash yoki xavfli holatlarni avtomatik ravishda bildiradigan tizimlarni joriy etish mumkin.

Kod tahlili

Quyida keltirilgan Python kodi, tarmoqni tahlil qilish va xavfsizlikni baholash uchun bir nechta funksiyalarni o‘z ichiga oladi. Ushbu kodning ishlash prinsiplarini va har bir funksiyasining qanday amalga oshirilishini batafsil tahlil qilamiz.

python

Копировать

def ssl\_analyzer(self, target):

context = ssl.create\_default\_context()

with socket.create\_connection((target, 443)) as sock:

with context.wrap\_socket(sock, server\_hostname=target) as ssock:

cert = ssock.getpeercert(binary\_form=True)

cert\_obj = x509.load\_der\_x509\_certificate(cert, default\_backend())

cert\_info = {

'issuer': cert\_obj.issuer.rfc4514\_string(),

'subject': cert\_obj.subject.rfc4514\_string(),

'version': cert\_obj.version,

'serial\_number': cert\_obj.serial\_number,

'not\_valid\_before': cert\_obj.not\_valid\_before.isoformat(),

'not\_valid\_after': cert\_obj.not\_valid\_after.isoformat(),

'signature\_algorithm': cert\_obj.signature\_algorithm\_oid.\_name

}

self.report\_data['ssl'] = cert\_info

**SSL Tahlili (ssl\_analyzer funksiyasi)**

Ushbu funksiya SSL sertifikatini tahlil qilish uchun mo‘ljallangan. SSL (Secure Sockets Layer) sertifikati, tizimga bog‘lanishdan oldin uning xavfsizligini tasdiqlash uchun ishlatiladi. Kodda quyidagi amallar bajariladi:

1. **SSL kontekstini yaratish**: ssl.create\_default\_context() funksiyasi SSL ulanishini yaratish uchun standarti o‘rnatadi.
2. **Socket yaratish**: socket.create\_connection() orqali tizimning 443-portiga (HTTPS uchun) ulanish o‘rnatiladi.
3. **SSL socket o‘rash**: context.wrap\_socket() yordamida socketni SSL konteksiga o‘rab, xavfsiz ulanishni ta'minlaydi.
4. **Sertifikatni olish**: getpeercert(binary\_form=True) yordamida serverning SSL sertifikati olinadi.
5. **Sertifikatni dekodlash**: x509.load\_der\_x509\_certificate() sertifikatni dekodlash va tizimning sertifikatini tahlil qilish imkonini beradi.
6. **Sertifikat ma'lumotlarini olish**: Sertifikatning chiqaruvchi va foydalanuvchi ma'lumotlari, amal qilish davri va imzo algoritmi kabi ma'lumotlar olinadi.
7. **Hisobot yaratish**: Ushbu ma'lumotlar self.report\_data['ssl'] obyektiga saqlanadi va foydalanuvchiga tahlil qilingan SSL sertifikati haqida ma'lumot taqdim etiladi.

python

def web\_crawler(self, url):

print(Fore.CYAN + f"\n[+] Web reconnaissance for {url}")

parsed = urlparse(url)

base\_url = f"{parsed.scheme}://{parsed.netloc}"

# Directory brute-forcing

with open('wordlist.txt', 'r') as f:

directories = f.read().splitlines()

discovered = []

for dir in directories:

full\_url = f"{base\_url}/{dir}"

try:

response = requests.get(full\_url, timeout=3)

if response.status\_code == 200:

discovered.append(full\_url)

print(Fore.GREEN + f"Found: {full\_url}")

except Exception as e:

continue

self.report\_data['web'] = {

'discovered\_paths': discovered,

'headers': dict(requests.get(base\_url).headers)

}

**Veb Tarmoqni Kashf Etish (web\_crawler funksiyasi)**

Bu funksiya, veb tarmog‘ini kashf etishga mo‘ljallangan. Veb saytning mavjud direktoriyalarini aniqlash va tahlil qilish uchun ishlatiladi. Jarayon quyidagi bosqichlardan iborat:

1. **URLni tahlil qilish**: urlparse(url) yordamida URL tarkibini tahlil qiladi va asosiy manzilni olish uchun parsed.scheme va parsed.netloc qiymatlaridan foydalanadi.
2. **So‘zlik bilan veb-directory brute-forcing**: wordlist.txt faylidan direktoriyalarni o‘qib, har bir direktoriyani tekshiradi. So‘zlikda har bir yo‘lni sinab ko‘radi.
3. **HTTP so‘rovi yuborish**: Har bir kiritilgan yo‘lga requests.get() orqali HTTP so‘rovi yuboriladi. Agar status kodi 200 bo‘lsa, demak, bu yo‘l mavjud va topildi.
4. **Ma'lumotlarni yig‘ish**: Topilgan yo‘llar va veb-saytning bosh sahifasidan olingan javoblar self.report\_data['web'] ga saqlanadi.

python

def generate\_report(self, filename):

with open(filename, 'w') as f:

json.dump(self.report\_data, f, indent=4)

print(Fore.GREEN + f"\n[+] Report generated: {filename}")

**Hisobotni Yaratish (generate\_report funksiyasi)**

Ushbu funksiya, tahlil qilingan ma'lumotlarni JSON formatida faylga yozadi va foydalanuvchiga hisobotni taqdim etadi. Hisobotni quyidagi tarzda yaratadi:

1. **JSON formatida saqlash**: json.dump() yordamida barcha tahlil qilingan ma'lumotlarni faylga saqlaydi. Bu ma'lumotlar SSL sertifikati, veb kashfiyot va boshqa tahlil natijalarini o‘z ichiga oladi.
2. **Faylni yaratish**: Hisobotni foydalanuvchiga ko‘rsatish uchun faylni yaratadi.

Python

def main():

parser = argparse.ArgumentParser(description="Advanced Reconnaissance Tool")

parser.add\_argument('-t', '--target', required=True)

parser.add\_argument('-p', '--ports', default='1-1024')

parser.add\_argument('-d', '--dns', action='store\_true')

parser.add\_argument('-w', '--web', action='store\_true')

parser.add\_argument('-s', '--ssl', action='store\_true')

parser.add\_argument('-o', '--output', default='report.json')

args = parser.parse\_args()

tool = AdvancedReconTool()

try:

# Port scanning

tool.advanced\_scan(args.target, args.ports)

# DNS enumeration

if args.dns:

tool.dns\_enumeration(args.target)

# SSL analysis

if args.ssl:

tool.ssl\_analyzer(args.target)

# Web reconnaissance

if args.web:

tool.web\_crawler(f"http://{args.target}")

tool.generate\_report(args.output)

except KeyboardInterrupt:

print(Fore.RED + "\n[!] Scan interrupted by user!")

sys.exit(1)

if \_\_name\_\_ == "\_\_main\_\_":

main()

**Asosiy Funksiya (main funksiyasi)**

Asosiy funksiya komandalar satri orqali foydalanuvchidan kiritilgan parametrlarni qabul qiladi va dasturga tegishli tahlil usullarini chaqiradi:

1. **Argparse moduli**: Bu modul foydalanuvchiga komandalar satridan parametrlarni kiritish imkonini beradi. Foydalanuvchi maqsadli tizim manzilini, portlar, DNS tahlili, SSL va veb kashfiyotni tanlashi mumkin.
2. **Tahlil metodlarini chaqirish**: Foydalanuvchi kiritgan parametrlar asosida ssl\_analyzer(), web\_crawler(), dns\_enumeration() va generate\_report() kabi metodlar chaqiriladi.

Dasturni ishga tushirish uchun namuna buyruq quyidagicha ko'rinishda bo'ladi:

python recon\_tool.py -t example.com -p 1-65535 -d -w -s -o full\_report.json

Bu buyruqning har bir qismi quyidagi funksiyalarni bajaradi:

**-t example.com**: Bu parametr dasturga tahlil qilinadigan manzilingizni ko'rsatadi. Misolda example.com domeni tanlangan.

**-p 1-65535**: Bu parametr tarmoq portlarini ko'rsatadi. Bu yerda barcha portlar (1 dan 65535 gacha) skanerlash uchun belgilangan.

**-d**: DNS tahlilini ishga tushiradi. Bu parametr yordamida tizimning DNS serveri haqida ma'lumot olish mumkin.

**-w**: Veb-resurslarni kashf qilish uchun parametrlash. Bu parametr orqali veb resurslar va direktoriyalarni aniqlash amalga oshiriladi.

**-s**: SSL sertifikati tahlilini ishga tushiradi. Bu parametr orqali SSL sertifikati tahlil qilinadi va tizim xavfsizligi haqida ma'lumot yig‘iladi.

**-o full\_report.json**: Bu parametr yordamida tahlil natijalari saqlanadigan fayl nomi va formatini belgilaysiz. Misolda full\_report.json fayl nomi bilan natija saqlanadi.

**Dasturni ishga tushirish:**

1. Python va kerakli kutubxonalar o'rnatilgan bo'lishi kerak.
2. Yuqoridagi buyruqni terminal yoki komandalar oynasida bajarishingiz mumkin.
3. recon\_tool.py faylini o'zingizning manzilingizga moslab ishga tushirishingiz kerak.

Natija sifatida, full\_report.json faylida tahlil qilingan tizim haqida batafsil hisobot saqlanadi.

**Xulosa**

Ushbu maqolada razvedka hujumlarini amalga oshirishga mo‘ljallangan dasturiy vosita ishlab chiqilishi va uning samaradorligi sinovdan o‘tkazildi. Maqsadimiz — tizimlarni va tarmoqlarni himoya qilish uchun zarur bo‘lgan dastlabki tahlil bosqichlarini avtomatlashtirish va xavfsizlikni mustahkamlashda yordam beradigan vositani ishlab chiqish edi. Olingan natijalar dasturiy vositaning tarmoq xavfsizligini aniqlashda va zaifliklarni oldini olishda samarali ekanligini ko‘rsatdi.

Dastur orqali amalga oshirilgan port skanerlash, DNS tahlili, SSL tahlili va veb resurslarni kashf etish jarayonlari, tizimning zaif joylarini aniqlashda va ularni to‘g‘rilashda yordam berdi. Bu esa, o‘z navbatida, kiberhujumlar va tizimga bo‘lgan tajovuzlarni oldini olish uchun muhim bosqich hisoblanadi. Eksperimentlar natijasida dastur yuqori tezlikda va aniqlikda ishlashini isbotladi, va foydalanuvchi uchun qulay interfeys orqali tizimning barcha xavfsizligini baholash imkoniyatini yaratdi.

Dastur, tizimlar va tarmoqlarni tahlil qilish uchun bir nechta usullarni birlashtirgan kuchli vosita hisoblanadi. SSL sertifikati tahlili, veb kashfiyot, DNS tahlili va port skanerlash kabi funksiyalar orqali tizimdagi zaifliklarni aniqlash imkonini beradi. Kodning har bir qismi, kiberxavfsizlikni ta'minlash uchun zarur bo‘lgan ma'lumotlarni to‘plash va tahlil qilishni osonlashtiradi. Bunday vositalar kiberxavfsizlik tahlilchilariga tizimlarni va tarmoq infratuzilmasini tekshirishda yordam beradi, ularning zaifliklarini aniqlashda samarali bo‘ladi.

Yakuniy tahlil va muhokama, dasturiy vositaning o‘ziga xos xususiyatlari va uning kiberxavfsizlikda ahamiyatini ko‘rsatdi. Razvedka hujumini amalga oshirishga mo‘ljallangan vosita yordamida tizimni xavfsizligini tekshirish va zaifliklarni aniqlash samarali amalga oshirildi. Eksperimentlar natijalaridan olingan tahlil, bu vositaning tizim xavfsizligini ta'minlashda muhim ahamiyatga ega ekanligini tasdiqladi. Kelajakda, ushbu vosita yanada rivojlantirilishi va avtomatik tahlil qilish imkoniyatlari bilan kengaytirilishi kerak. Bu esa tizimlarni himoya qilishda yanada yuqori samaradorlikni ta'minlaydi.

Shu tarzda, tarmoq xavfsizligini va tizimlarni himoya qilishda foydalaniladigan dasturiy vosita ishlab chiqildi va sinovdan o‘tkazildi. Dastur yordamida tarmoqdagi va tizimdagi zaifliklar aniqlandi va bu, o‘z navbatida, tizim xavfsizligini ta'minlash uchun muhim qadamdir. Kelajakda ushbu vositani yanada rivojlantirish, tahlil qilishni avtomatlashtirish va yangi xavfsizlikni kuzatish tizimlarini joriy etish zarur bo‘ladi. Bu, kiberxavfsizlikni ta'minlashda yanada yuqori samaradorlikka erishish imkonini beradi.

Foydalanilgan adabiyotlar

1.Mitnick, K. (2017). *The Art of Invisibility*. Skyhorse Publishing.

2.McClure, S., Scambray, J. (2020). *Hacking Exposed*. McGraw-Hill Education.

Kali Linux Documentation. (https://www.kali.org/docs/)

3.OWASP Foundation. (2021). *OWASP Top 10 – 2021*. (https://owasp.org/www-project-top-ten/)

4.Python Software Foundation. (2021). *Python Documentation*. (<https://docs.python.org/3/>)

**Eslatma**:Ushbu maqola sertifikat olish uchun so’rov yuborildi.Sertifikat 2,3 kunda yuboriladi.