HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

THE PRINCIPLE AND CAPABILITIES OF THE COWRIE HONEYPOT SYSTEM

Khorozov Khumoyun Inomjon oglu,

Baliyev Firdavs Azimjonovich,

Mamatkarimov Asadbek Anvarjonovich,

Qaxramonov Sardor

Students of TUIT, Cybersecurity faculty

Doi" https://doi.org/10.5281/zenodo.21756179

Abstract: This article analyzes the operating principle, architecture, and role of the Cowrie honeypot system in providing modern cybersecurity. The Cowrie system allows attracting cyberattackers, tracking their movements, as well as analyzing attack methods by emulating SSH and Telnet services. During the study, the capabilities of the Cowrie honeypot to record the authentication process, record commands, monitor file upload activity, and analyze log data were explored. The obtained results indicate that the Cowrie system is an effective tool for early detection of cyberattacks, collecting information about threats, and improving the security of information systems.

Keywords: Cowrie honeypot, honeypot, SSH, Telnet, cybersecurity, cyberattack, network monitoring, information security, threat detection, malicious activities.

COWRIE HONEYPOT TIZIMINING ISHLASH PRINSIPI VA IMKONIYATLARI

Kalit so‘zlar: Cowrie honeypot, honeypot, SSH, Telnet, kiberxavfsizlik, kiberhujum, tarmoq monitoringi, axborot xavfsizligi, tahdidlarni aniqlash, zararli faoliyat.

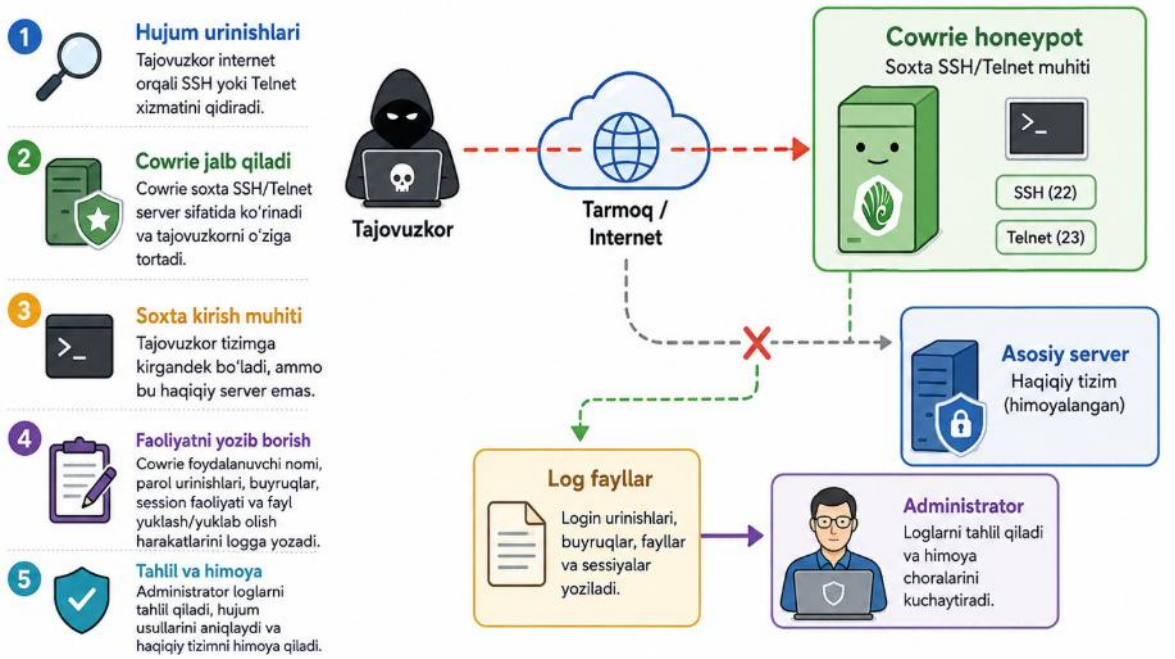
Annotatsiya: Mazkur maqolada Cowrie honeypot tizimining ishlash prinsipi, arxitekturasi va zamonaviy kiberxavfsizlikni ta'minlashdagi o‘rni tahlil qilingan. Cowrie tizimi SSH va Telnet xizmatlarini emulyatsiya qilish orqali kiberhujumchilarni jalb etish, ularning harakatlarini kuzatish hamda hujum usullarini tahlil qilish imkonini beradi. Tadqiqot davomida Cowrie honeypotining autentifikatsiya jarayonini qayd etish, buyruqlarni yozib borish, fayl yuklash faoliyatini nazorat qilish va jurnal ma'lumotlarini tahlil qilish imkoniyatlari o‘rganilgan. Olingan natijalar Cowrie tizimining kiberhujumlarni erta aniqlash, tahdidlar haqida ma'lumot to‘plash hamda axborot tizimlari xavfsizligini oshirishda samarali vosita ekanligini ko‘rsatadi.

Cowrie honeypot tizimi SSH va Telnet xizmatlariga qaratilgan hujumlarni kuzatish, qayd etish va tahlil qilish uchun mo‘ljallangan maxsus kiberxavfsizlik vositasidir. U haqiqiy serverga o‘xshash muhit yaratib, tajovuzkorlarni o‘ziga jalb qiladi va ularning barcha harakatlarini nazorat ostida yozib boradi. Cowrie asosan SSH va Telnet orqali amalga oshiriladigan brute-force, dictionary attack, credential stuffing, port scanning va ruxsatsiz kirish urinishlarini o‘rganishda keng qo‘llaniladi. Shu sababli u kiberxavfsizlik tadqiqotlari, laboratoriya ishlari va real hujumlarni monitoring qilishda muhim amaliy vosita hisoblanadi.

Cowrie honeypotning asosiy vazifasi tajovuzkorni haqiqiy tizimga kirgandek his qildirishdir. Ya’ni hujumchi SSH yoki Telnet orqali tizimga ulanishga harakat qiladi, login va parol kiritadi, keyin

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

esa go‘yoki server terminaliga tushgandek bo‘ladi. Aslida esa u haqiqiy serverda emas, balki Cowrie tomonidan yaratilgan nazorat ostidagi soxta terminal muhitida ishlayotgan bo‘ladi. Bu yondashuv hujumchining faoliyatini xavfsiz tarzda kuzatish imkonini beradi.



1.6-rasm. Cowrie honeypot tizimining ishlash prinsipi

Cowrie honeypot odatda medium-interaction honeypot turiga kiradi. Chunki u hujumchiga oddiy low-interaction honeypotlarga qaraganda ko‘proq o‘zaro aloqa imkonini beradi. Hujumchi terminalda buyruqlar kiritishi, kataloglarni ko‘rishga urinishi, fayllar bilan ishlashga harakat qilishi mumkin. Biroq Cowrie to‘liq haqiqiy operatsion tizim emas. U faqat haqiqiy tizimga o‘xshash muhitni taqlid qiladi. Shu sababli u high-interaction honeypotlarga qaraganda xavfsizroq hisoblanadi.

Cowrie tizimining ishlash prinsipi bir necha bosqichdan iborat. Birinchi bosqichda Cowrie serverda SSH yoki Telnet xizmatiga o‘xshash xizmatni ishga tushiradi. Odatda haqiqiy SSH xizmati 22-portda ishlaydi, Cowrie esa xavfsizlik maqsadida boshqa portda ishga tushirilishi mumkin. Keyinchalik tarmoq sozlamalari yordamida tashqi foydalanuvchilar 22-portga murojaat qilganda ularning so‘rovlari Cowrie xizmatiga yo‘naltiriladi. Natijada tajovuzkor haqiqiy SSH serverga ulanayotganini o‘ylaydi.

Ikkinchi bosqichda tajovuzkor autentifikatsiya jarayonidan o‘tishga urinadi. Bu jarayonda u foydalanuvchi nomi va parol kiritadi. Cowrie esa kiritilgan barcha login va parollarni yozib boradi. Masalan, hujumchi root:123456, admin:admin, user:password, test:test kabi kombinatsiyalarni sinab ko‘rishi mumkin. Cowrie bu ma’lumotlarni log fayllarda saqlaydi. Keyinchalik ushbu loglar tahlil qilinib, eng ko‘p ishlatilgan login va parollar aniqlanadi.

Uchinchi bosqichda Cowrie hujumchini soxta terminal muhitiga kiritishi mumkin. Bunda hujumchi o‘zini tizimga muvaffaqiyatli kirgandek his qiladi. Terminalda buyruqlar yozadi, kataloglarni ko‘radi, tizim haqida ma’lumot olishga urinadi. Cowrie esa bu buyruqlarning barchasini qayd etadi. Masalan, hujumchi ls, pwd, whoami, uname -a, id, cat /etc/passwd, wget, curl kabi

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

buyruqlarni ishlatishi mumkin. Bunday buyruqlar hujumchining maqsadi va uslubini tushunishga yordam beradi.

Cowrie honeypotning eng muhim imkoniyatlaridan biri SSH hujumlarini qayd etishdir. Internetga ochiq SSH xizmatlari ko‘pincha avtomatlashtirilgan botlar tomonidan skaner qilinadi va ularga brute-force yoki dictionary attack hujumlari amalga oshiriladi. Cowrie bunday hujumlarni aniqlab, ularning vaqti, manbasi, ishlatilgan login-parollar va ulanish tafsilotlarini saqlaydi. Bu ma’lumotlar orqali SSH xizmatiga qaratilgan hujumlarning intensivligi va xususiyatlari o‘rganiladi.

Telnet hujumlarini qayd etish ham Cowrie tizimining muhim imkoniyatlaridan biridir. Telnet eski va xavfsizligi past protokol bo‘lib, unda ma’lumotlar shifrlanmagan holatda uzatiladi. Hozirgi kunda Telnetdan foydalanish xavfsizlik nuqtayi nazaridan tavsiya etilmaydi, lekin ayrim eski qurilmalar va IoT tizimlarida u hali ham uchraydi. Tajovuzkorlar Telnet xizmatlari orqali zaif qurilmalarga kirishga urinadilar. Cowrie esa bunday urinishlarni ham qayd etib, Telnet orqali amalga oshiriladigan hujumlarni tahlil qilish imkonini beradi.

Cowrie honeypot soxta terminal muhiti yaratish orqali hujumchini uzoqroq vaqt davomida kuzatishga imkon beradi. Agar honeypot faqat login-parol urinishlarini qayd etsa, hujumchining tizimga kirgandan keyingi xatti-harakatlari noma’lum bo‘lib qoladi. Cowrie esa tajovuzkorga terminalga kirgandek imkon yaratadi. Natijada hujumchi keyingi bosqichlarda qanday buyruqlarni bajarishi, qanday ma’lumotlarni izlashga urinishi va qanday zararli fayllarni yuklab olishga harakat qilishi aniqlanadi.

Soxta terminal muhitida hujumchi odatda avval tizim haqida umumiy ma’lumot olishga harakat qiladi. Masalan, uname -a buyrug‘i orqali operatsion tizim va yadro versiyasini bilishga urinadi. whoami buyrug‘i orqali qaysi foydalanuvchi nomi bilan tizimga kirganini tekshiradi. id buyrug‘i orqali foydalanuvchi huquqlarini ko‘radi. pwd va ls buyruqlari yordamida joriy katalog va fayllar ro‘yxatini tekshiradi. Cowrie bu harakatlarning barchasini saqlab boradi.

Cowrie honeypot login-parol urinishlarini yozib borish imkoniyati bilan ham juda foydalidir. SSH hujumlarida tajovuzkorlar ko‘pincha oldindan tayyorlangan login-parol ro‘yxatlaridan foydalanadilar. Cowrie yordamida bu ro‘yxatlarda qaysi foydalanuvchi nomlari va parollar ko‘p uchrashini aniqlash mumkin. Masalan, “root”, “admin”, “oracle”, “ubuntu”, “user”, “test” kabi loginlar, “123456”, “password”, “admin123”, “qwerty”, “root” kabi parollar ko‘p sinab ko‘rilishi mumkin.

Login-parol urinishlarini tahlil qilish real serverlar xavfsizligini kuchaytirish uchun muhim ahamiyatga ega. Agar honeypot loglarida ma’lum bir foydalanuvchi nomiga ko‘p hujum qilinayotgani aniqlansa, real tizimlarda shu foydalanuvchi nomlaridan foydalanishni cheklash yoki ularni kuchli autentifikatsiya bilan himoyalash mumkin. Shuningdek, zaif parollar ro‘yxatini shakllantirib, tashkilot ichida bunday parollardan foydalanishni taqiqlash mumkin.

Cowrie honeypot buyruqlarni saqlash imkoniyatiga ham ega. Hujumchi soxta terminalda qanday buyruq yozsa, Cowrie uni vaqt belgisi bilan log faylga saqlaydi. Bu juda muhim, chunki buyruqlar hujumchining niyatini ko‘rsatadi. Masalan, agar hujumchi cat /etc/passwd buyrug‘ini ishlatsa, u tizim foydalanuvchilari haqida ma’lumot olishga urinayotgan bo‘lishi mumkin. Agar wget yoki curl buyruqlaridan foydalansa, u tashqi manbadan zararli fayl yuklamoqchi bo‘lishi ehtimoli bor.

Cowrie zararli fayllarni yuklab olish urinishlarini ham qayd etishi mumkin. Masalan, tajovuzkor internetdagi serverdan skript yoki bajariluvchi fayl yuklab olishga harakat qiladi. Cowrie bunday

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

fayllarni xavfsiz muhitda saqlab, keyinchalik tahlil qilish imkonini beradi. Bu orqali zararli dasturlarning turi, ularning manbasi va qanday vazifani bajarishga mo‘ljallangani haqida ma’lumot olish mumkin. Biroq bunday fayllar bilan ishlashda ehtiyotkorlik talab etiladi, chunki ular zararli bo‘lishi mumkin.

Cowrie tizimining yana bir muhim imkoniyati IP-manzillarni aniqlashdir. Har bir ulanishda hujumchining IP-manzili log faylga yoziladi. Bu IP-manzillar orqali hujum manbalari, ularning geografik joylashuvi, takroriy urinishlar soni va hujumlar vaqti tahlil qilinadi. Masalan, bir IP-manzildan qisqa vaqt ichida yuzlab login-parol urinishlari bo‘lsa, bu brute-force hujumidan dalolat beradi. Turli IP-manzillardan bir xil parollar sinab ko‘rilsa, bu botnet yoki taqsimlangan hujum belgisi bo‘lishi mumkin.

IP-manzillarni tahlil qilish xavfsizlik monitoringida muhim ahamiyatga ega. Honeypot orqali aniqlangan zararli IP-manzillar keyinchalik firewall yoki IDS/IPS tizimlarida bloklash ro‘yxatiga qo‘shilishi mumkin. Shuningdek, bu ma’lumotlar SIEM tizimlariga yuborilib, boshqa xavfsizlik hodisalari bilan solishtirilishi mumkin. Masalan, honeypotga hujum qilgan IP-manzil keyinchalik real serverga ham ulanishga urinsa, bu jiddiy ogohlantirish sifatida baholanadi.

Cowrie log fayllar bilan ishlash imkoniyatlari orqali hujumlarni chuqur tahlil qilishga yordam beradi. Cowrie odatda har bir hodisani alohida yozib boradi. Loglarda ulanish vaqti, sessiya identifikatori, IP-manzil, kiritilgan login va parol, bajarilgan buyruqlar, yuklab olish urinishlari va sessiya yakuni haqidagi ma’lumotlar bo‘ladi. Bu loglar matn ko‘rinishida yoki JSON formatida saqlanishi mumkin. JSON formatidagi loglar keyinchalik avtomatik tahlil qilish, grafiklar yaratish yoki SIEM tizimlariga uzatish uchun qulay hisoblanadi.

Log fayllar bilan ishlashda eng muhim vazifalardan biri ularni tartibga solish va tahlil qilishdir. Masalan, bir kunlik loglarda minglab kirish urinishlari bo‘lishi mumkin. Ularni qo‘lda ko‘rib chiqish qiyin. Shu sababli loglarni filtrlash, guruhlash va statistik tahlil qilish zarur bo‘ladi. Masalan, eng ko‘p hujum qilgan IP-manzillar, eng ko‘p ishlatilgan loginlar, eng ko‘p sinab ko‘rilgan parollar, eng ko‘p bajarilgan buyruqlar va hujumlarning vaqt bo‘yicha taqsimoti aniqlanadi.

Cowrie honeypot orqali olingan ma’lumotlar diplom loyiha ishida amaliy tahlil uchun juda qulaydir. Masalan, tajriba sifatida Cowrie serverga o‘rnatiladi va ma’lum vaqt davomida internet orqali kelayotgan SSH urinishlari kuzatiladi. Keyin log fayllar yig‘iladi va tahlil qilinadi. Tahlil natijasida qaysi IP-manzillar faol bo‘lganligi, qaysi login-parollar ko‘p ishlatilganligi, hujumchilar qanday buyruqlar bajargani va qanday zararli fayllarni yuklashga uringani ko‘rsatiladi.

Cowrie tizimi hujumchilarning ish uslubini tushunishga yordam beradi. Masalan, ba’zi tajovuzkorlar tizimga kirgandan so‘ng darhol tizim ma’lumotlarini tekshiradi. Boshqalari esa birinchi navbatda zararli fayl yuklashga urinadi. Yana ayrimlari foydalanuvchi huquqlarini oshirishga yoki tizimdagi fayllarni o‘rganishga harakat qiladi. Cowrie bu harakatlarni bosqichma-bosqich yozib boradi. Natijada hujumchining harakat modeli shakllantiriladi.

Cowrie honeypotning afzalliklaridan biri shundaki, u real server xavfsizligiga zarar yetkazmasdan hujumlarni o‘rganish imkonini beradi. Haqiqiy ishlab turgan serverga hujumchini kiritish xavfli bo‘lishi mumkin. Chunki u maxfiy ma’lumotlarni o‘g‘irlashi yoki tizimni buzishi ehtimoli bor. Cowrie esa nazorat ostidagi muhit yaratadi va hujumchini haqiqiy tizimdan ajratib turadi. Shu sababli u amaliy tahlil uchun xavfsizroq vosita hisoblanadi.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

Yana bir afzalligi — Cowrie turli formatlarda ma’lumot saqlashi va boshqa tizimlar bilan integratsiya qilinishi mumkin. Masalan, loglarni SIEM tizimlari, Elasticsearch, Kibana yoki boshqa monitoring vositalari bilan ishlatish mumkin. Bu esa hujumlarni grafik ko‘rinishda tahlil qilish, diagrammalar yaratish va xavfsizlik holatini vizual kuzatish imkonini beradi. Diplom loyiha ishida ham Cowrie loglari asosida jadvallar, grafiklar va statistik tahlillar tuzish mumkin.

1.1-jadval

Cowrie tizimi orqali amaliy ma’lumotlarni olish

Tahlil qilinadigan ma’lumot	**Cowrie orqali olinadigan natija**
Login urinishlari	Hujumchi qaysi foydalanuvchi nomlarini sinagani aniqlanadi
Parol urinishlari	Eng ko‘p ishlatilgan zaif parollar ro‘yxati shakllanadi
IP-manzillar	Hujum manbalari va takroriy urinishlar aniqlanadi
Buyruqlar	Hujumchi tizimga kirgandan keyingi harakatlari ko‘riladi
Fayl yuklashlar	Zararli fayl yoki skript yuklash urinishlari aniqlanadi
Vaqt statistikasi	Hujumlar qaysi vaqt oralig‘ida ko‘paygani tahlil qilinadi

Cowrie honeypotning imkoniyatlari ko‘p bo‘lsa-da, undan foydalanishda ayrim ehtiyot choralariga rioya qilish zarur. Birinchidan, honeypot real ishlab turgan muhim serverlar bilan bir xil tarmoqda xavfsiz izolyatsiyasiz joylashtirilmasligi kerak. Ikkinchidan, honeypot orqali yuklangan zararli fayllar bevosita ishga tushirilmasligi lozim. Uchinchi tomondan, log fayllar muntazam tekshirilib borilishi kerak. Aks holda, Cowrie ko‘p ma’lumot yig‘adi, lekin bu ma’lumotlar foydali tahlilga aylantirilmaydi.

Cowrie tizimining yana bir muhim jihati shundaki, u o‘quv va ilmiy maqsadlarda juda qulaydir. Talabalar va tadqiqotchilar Cowrie yordamida real hujumlarni kuzatib, kiberxavfsizlik bo‘yicha amaliy bilimga ega bo‘ladilar. Masalan, SSH brute-force hujumi qanday ko‘rinishda logga tushishi, tajovuzkor qanday login-parollarni sinashi, tizimga kirgach qanday buyruqlarni bajarishi amalda o‘rganiladi. Bu esa nazariy bilimlarni real tahlil bilan mustahkamlaydi.

Cowrie honeypotdan olingan ma’lumotlar asosida xavfsizlik tavsiyalarini ishlab chiqish mumkin. Masalan, agar tahlilda “root” foydalanuvchisiga juda ko‘p hujum bo‘layotgani aniqlansa, real SSH serverlarda root orqali kirishni taqiqlash tavsiya etiladi. Agar oddiy parollar ko‘p sinab ko‘rilsa, kuchli parol siyosatini joriy etish kerakligi ko‘rsatiladi. Agar ma’lum IP-manzillar ko‘p hujum qilsa, firewall orqali ularni bloklash yoki monitoring ro‘yxatiga kiritish mumkin.

Cowrie tizimi hujumlarni faqat qayd etibgina qolmay, balki ularni tushunish uchun zarur ma’lumotlarni ham beradi. Bu jihati bilan u oddiy log monitoring vositalaridan farq qiladi. Oddiy SSH server loglarida asosan muvaffaqiyatsiz kirish urinishlari ko‘rinadi. Cowrie esa hujumchi tizimga kirgandan keyingi xatti-harakatlarini ham yozib boradi. Shu sababli u hujum zanjirini to‘liqroq ko‘rishga imkon beradi.

SSH va Telnet xizmatlariga qaratilgan hujumlar ko‘pincha avtomatlashtirilgan botlar yordamida amalga oshiriladi. Bunday botlar internetdagi ochiq portlarni topadi, ularga ulanadi va oldindan tayyorlangan login-parol ro‘yxatini sinab ko‘radi. Cowrie bunday jarayonlarni aniq qayd etadi. Agar

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

bir xil login-parollar turli IP-manzillardan qayta-qayta sinab ko‘rilsa, bu botnet faoliyatidan dalolat berishi mumkin. Bunday ma’lumotlar global kiberhujum tendensiyalarini tushunishda foydali bo‘ladi.

Cowrie loglarida saqlangan ma’lumotlardan hisobot tayyorlashda ham foydalanish mumkin. Masalan, diplom loyiha ishida quyidagi ko‘rsatkichlar jadval yoki grafik shaklida berilishi mumkin: umumiy ulanishlar soni, muvaffaqiyatsiz login urinishlari soni, eng faol IP-manzillar, eng ko‘p ishlatilgan foydalanuvchi nomlari, eng ko‘p sinab ko‘rilgan parollar, eng ko‘p bajarilgan buyruqlar va hujumlarning kunlik yoki soatlik taqsimoti. Bu natijalar mavzuning amaliy ahamiyatini ko‘rsatadi.

Cowrie honeypot tizimining ishlashida log fayllar asosiy axborot manbai hisoblanadi. Loglar orqali har bir sessiya alohida o‘rganiladi. Sessiya — bu hujumchining honeypotga ulangan vaqtidan boshlab chiqib ketgunigacha bo‘lgan jarayondir. Har bir sessiyada login-parol urinishlari, muvaffaqiyatli kirish holati, buyruqlar, fayl yuklashlar va ulanish tugashi haqidagi ma’lumotlar bo‘ladi. Sessiyalarni tahlil qilish orqali individual hujum ssenariysi aniqlanadi.

Cowrie tizimida buyruqlar tarixini saqlash hujumchilarning keyingi harakatlarini tushunishda juda muhimdir. Masalan, hujumchi tizimga kirgandan so‘ng cd /tmp buyrug‘ini bajarishi va keyin wget orqali fayl yuklashga urinishi mumkin. Bu ko‘pincha zararli skriptni vaqtinchalik katalogga yuklab, uni ishga tushirishga tayyorgarlik belgisi bo‘ladi. Agar bunday harakatlar ko‘p takrorlansa, bu ma’lum turdagi avtomatlashtirilgan hujum ssenariysini ko‘rsatadi.

Cowrie tizimida qayd etilgan IP-manzillarni qo‘shimcha tahlil qilish orqali hujum geografiyasi haqida ham xulosa qilish mumkin. Bunda IP-manzillar mamlakatlar bo‘yicha guruhlanadi. Albatta, IP-manzil har doim hujumchining haqiqiy joylashuvini aniq ko‘rsatmaydi, chunki tajovuzkor VPN, proksi yoki buzilgan boshqa serverlardan foydalanishi mumkin. Shunga qaramay, IP-manzillar hujum manbalarini umumiy baholash uchun foydali hisoblanadi.

Cowrie honeypot tizimidan foydalanishda monitoring jarayoni uzluksiz bo‘lishi kerak. Chunki SSH hujumlari har kuni va har xil vaqtda sodir bo‘lishi mumkin. Ba’zan hujumlar kechasi ko‘payadi, ba’zan esa botlar doimiy ravishda portlarni skanerlab turadi. Uzoqroq muddat davomida yig‘ilgan loglar qisqa muddatli loglarga qaraganda aniqroq tahlil beradi. Shuning uchun diplom loyiha ishida Cowrie’ni ma’lum vaqt davomida ishlatib, keyin natijalarni solishtirish maqsadga muvofiqdir.

Cowrie honeypot real serverlarni bevosita himoya qiluvchi vosita emas, balki hujumlarni kuzatish va tahlil qilish vositasidir. U firewall yoki antivirus kabi hujumni to‘g‘ridan-to‘g‘ri to‘xtatmaydi. Biroq u orqali olingan ma’lumotlar asosida real himoya choralarini kuchaytirish mumkin. Masalan, xavfli IP-manzillarni bloklash, zaif parollarni taqiqlash, root loginni o‘chirish, SSH kalitlari asosidagi autentifikatsiyani joriy etish va kirish urinishlarini cheklash kabi choralar ishlab chiqiladi. Cowrie honeypot tizimining kiberxavfsizlikdagi o‘rni aynan uning tahliliy imkoniyatlari bilan belgilanadi. U tajovuzkorlar qanday ishlashini, qaysi vositalardan foydalanishini va tizimga kirgandan keyin qanday harakat qilishini ko‘rsatib beradi. Bu esa xavfsizlik mutaxassislariga nazariy taxminlar emas, balki real hujumlar asosida qaror qabul qilish imkonini beradi.

Xulosa qilib aytganda, Cowrie honeypot SSH va Telnet hujumlarini o‘rganish uchun qulay, xavfsiz va samarali vositadir. U soxta terminal muhiti yaratadi, login-parol urinishlarini yozib boradi, hujumchilarning buyruqlarini saqlaydi, IP-manzillarni aniqlaydi va log fayllar orqali chuqur tahlil qilish imkonini beradi. Cowrie yordamida olingan ma’lumotlar real serverlar xavfsizligini kuchaytirish, hujumchilar faoliyatini tushunish va diplom loyiha ishining amaliy qismini asoslashda muhim ahamiyatga ega. Shu sababli “Cowrie honeypot asosida SSH xizmatiga qilingan hujumlarni

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

monitoring va tahlil qilish” mavzusida Cowrie tizimining ishlash prinsipi va imkoniyatlarini o‘rganish asosiy nazariy yo‘nalishlardan biri hisoblanadi.

Xulosa

Tadqiqot natijalari shuni ko‘rsatdiki, Cowrie honeypot tizimi SSH va Telnet xizmatlariga qaratilgan kiberhujumlarni aniqlash hamda tahlil qilish uchun samarali yechim hisoblanadi. Tizim hujumchilar tomonidan amalga oshiriladigan autentifikatsiya urinishlari, bajarilgan buyruqlar, yuklangan fayllar va boshqa faoliyatlarni batafsil qayd etadi. Bu ma'lumotlar yangi tahdidlarni aniqlash, hujum usullarini tahlil qilish va axborot tizimlarini himoyalash strategiyasini takomillashtirish imkonini beradi. Bundan tashqari, Cowrie honeypot tizimini SIEM platformalari, IDS/IPS vositalari va log tahlil tizimlari bilan integratsiya qilish orqali real vaqt rejimida monitoringni tashkil etish hamda tahdidlarga tezkor javob berish mumkin. Kelgusida sun'iy intellekt va mashinali o‘qitish algoritmlarini Cowrie tizimiga integratsiya qilish hujumlarni avtomatik tasniflash va prognozlash imkoniyatlarini yanada kengaytiradi. Shu sababli, Cowrie honeypot texnologiyasi davlat tashkilotlari, korporativ tarmoqlar va ilmiy-tadqiqot muassasalarida kiberxavfsizlikni ta'minlashning muhim vositalaridan biri sifatida tavsiya etiladi.

Foydalanilgan adabiyotlar

1. Oosterhof M. **Cowrie SSH/Telnet Honeypot Project**. GitHub Repository, 2025.
2. Spitzner L. *Honeypots: Tracking Hackers*. Addison-Wesley, 2003.
3. Provos N., Holz T. *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Addison-Wesley, 2008.
4. NIST. *Guide to Intrusion Detection and Prevention Systems (SP 800-94)*. National Institute of Standards and Technology, 2007.
5. RFC 4251. *The Secure Shell (SSH) Protocol Architecture*. IETF, 2006.
6. RFC 4253. *The Secure Shell (SSH) Transport Layer Protocol*. IETF, 2006.
7. ENISA. *Threat Landscape Report*. European Union Agency for Cybersecurity, 2024.
8. Stallings W. *Cryptography and Network Security: Principles and Practice*. 8th Edition. Pearson, 2023.
9. Anderson R. *Security Engineering*. 3rd Edition. Wiley, 2020.
10. CISA. *Cybersecurity Best Practices*. Cybersecurity and Infrastructure Security Agency, 2024.