BG Pulse Journal USA
ISSN:1947-2536 http://www.bgpulseusa.com/index.php/bg

HONEYPOT TECHNOLOGIES AND THEIR ROLE IN CYBERSECURITY

Khorozov Khumoyun Inomjon oglu,

Baliyev Firdavs Azimjonovich,

Qaxramonov Sardor,

Sotvoldiyev Asadbek

Students of TUIT, Cybersecurity faculty

Doi: https://doi.org/10.5281/zenodo.21766235

Abstract: This article analyzes the role and importance of honeypot technologies in cybersecurity. The principle of operation of honeypot systems, their types and capabilities in detecting and analyzing the activities of cybercriminals are highlighted. It also discusses ways to identify vulnerabilities in network infrastructure through the use of honeypot technologies, study new types of cyberattacks, and increase the level of protection of information systems. The results of the study suggest that honeypot systems are an important tool for improving cybersecurity monitoring and developing effective defenses against modern threats.

Keywords: Honeypot, cybersecurity, network security, cyberattack, malware, network monitoring, threat detection, IDS, IPS, information security.

HONEYPOT TEXNOLOGIYALARI VA ULARNING KIBERXAVFSIZLIKDAGI O‘RNI

Annotatsiya: Mazkur maqolada honeypot texnologiyalarining kiberxavfsizlikni ta'minlashdagi o‘rni va ahamiyati tahlil qilingan. Honeypot tizimlarining ishlash prinsipi, ularning turlari hamda kiberjinoyatchilar faoliyatini aniqlash va tahlil qilishdagi imkoniyatlari yoritilgan. Shuningdek, honeypot texnologiyalaridan foydalanish orqali tarmoq infratuzilmasidagi zaifliklarni aniqlash, yangi turdagi kiberhujumlarni o‘rganish va axborot tizimlarining himoya darajasini oshirish usullari ko‘rib chiqilgan. Tadqiqot natijalari honeypot tizimlari kiberxavfsizlik monitoringini takomillashtirish va zamonaviy tahdidlarga qarshi samarali himoya choralarini ishlab chiqishda muhim vosita ekanligini ko‘rsatadi.

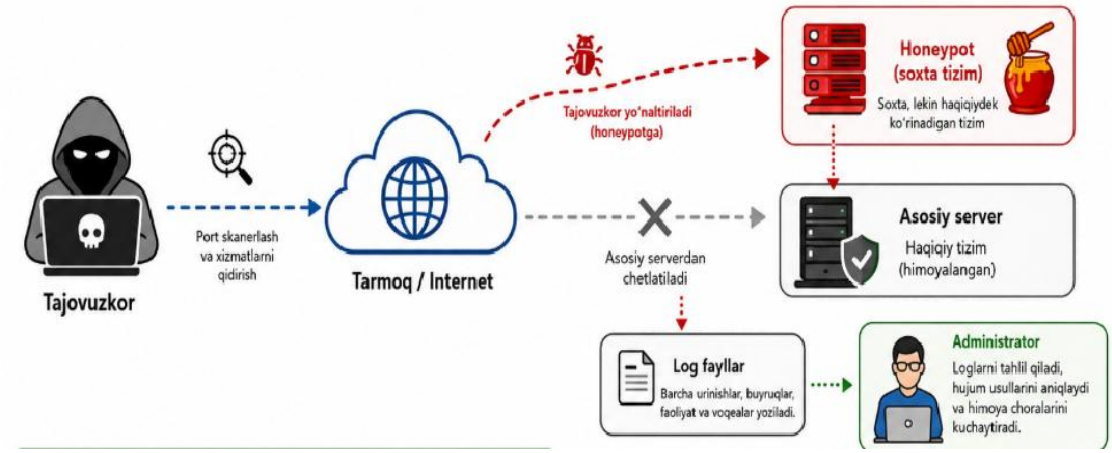
Kalit so‘zlar: Honeypot, kiberxavfsizlik, tarmoq xavfsizligi, kiberhujum, zararli dastur, tarmoq monitoringi, tahdidlarni aniqlash, IDS, IPS, axborot xavfsizligi.

Zamonaviy axborot tizimlarida kiberxavfsizlikni ta’minlash faqatgina antivirus, firewall yoki oddiy himoya vositalaridan foydalanish bilan cheklanib qolmaydi. Bugungi kunda kiberhujumlar tobora murakkablashib, avtomatlashtirilgan botlar, zararli dasturlar, parol tanlash hujumlari, tarmoqni skanerlash, fishing va ruxsatsiz kirish urinishlari orqali amalga oshirilmoqda. Shu sababli tashkilotlar nafaqat hujumlarni to‘xtatish, balki ularni oldindan aniqlash, hujumchilarning usullarini

o‘rganish va xavfsizlik choralarini kuchaytirishga ham alohida e’tibor qaratmoqda. Ana shunday maqsadlarda qo‘llaniladigan samarali texnologiyalardan biri honeypot texnologiyasi hisoblanadi.

Honeypot — bu tajovuzkorlarni o‘ziga jalb qilish, ularning xatti-harakatlarini kuzatish, hujum usullarini tahlil qilish va kiberxavfsizlik bo‘yicha foydali ma’lumotlar yig‘ish uchun maxsus yaratilgan sun’iy yoki nazorat ostidagi axborot tizimidir. Oddiy qilib aytganda, honeypot haqiqiy server yoki xizmatga o‘xshab ko‘rinadi, biroq uning asosiy vazifasi real foydalanuvchilarga xizmat ko‘rsatish emas, balki hujumchilarni aniqlash va ularning faoliyatini qayd etishdan iborat.

Honeypot texnologiyasi “aldamchi nishon” vazifasini bajaradi. Tajovuzkor internet orqali ochiq portlarni skanerlashi, zaif parollarni sinab ko‘rishi yoki tizimga kirishga urinishi mumkin. Agar u honeypotga duch kelsa, uni haqiqiy tizim deb o‘ylaydi va hujumni davom ettiradi. Shu jarayonda honeypot hujumchining IP-manzili, ishlatgan login va parollari, bajargan buyruqlari, yuklab olgan fayllari, ulanish vaqti va boshqa muhim ma’lumotlarni yozib boradi. Natijada xavfsizlik mutaxassislari hujumchilar qanday usullardan foydalanayotganini aniq ko‘ra oladilar.



1.1-rasm. Honeypot texnologiyasining ishlash prinsipi

Honeypot texnologiyalarining kiberxavfsizlikdagi ahamiyati juda katta. Chunki an’anaviy himoya vositalari, masalan, firewall yoki IDS/IPS tizimlari asosan ma’lum qoidalar va imzolar asosida ishlaydi. Ya’ni ular oldindan ma’lum bo‘lgan hujumlarni aniqlashda samarali bo‘lishi mumkin. Honeypot esa hujumchining real xatti-harakatlarini kuzatishga imkon beradi. Bu orqali yangi hujum usullari, noma’lum zararli dasturlar va avtomatlashtirilgan botlar faoliyati haqida amaliy ma’lumot olish mumkin.

Honeypotlar odatda haqiqiy ishlab turgan tizimlardan ajratilgan holda tashkil etiladi. Buning sababi shundaki, honeypotga hujum qilgan tajovuzkor real tarmoqqa zarar yetkazmasligi kerak. Agar honeypot noto‘g‘ri sozlansa yoki real tizimlar bilan bevosita bog‘langan bo‘lsa, u xavfsizlik uchun qo‘shimcha xavf tug‘dirishi mumkin. Shu sababli honeypotlarni yaratishda izolyatsiya, monitoring, loglash va nazorat mexanizmlariga alohida e’tibor beriladi.

Honeypot texnologiyalarini turli mezonlar asosida tasniflash mumkin. Ularning eng keng tarqalgan tasnifi o‘zaro ta’sir darajasiga ko‘ra bo‘linishidir. Bunga ko‘ra honeypotlar asosan low-

interaction, medium-interaction va high-interaction honeypotlarga ajratiladi. Har bir tur o‘ziga xos imkoniyat, afzallik va kamchiliklarga ega.

Low-interaction honeypot — bu hujumchi bilan cheklangan darajada o‘zaro aloqaga kirishadigan honeypot turidir. Bunday honeypotlar odatda haqiqiy operatsion tizim yoki to‘liq xizmatni ishga tushirmaydi, balki ma’lum xizmatlarning soddalashtirilgan ko‘rinishini taqlid qiladi. Masalan, SSH, FTP, HTTP yoki Telnet xizmatlari oddiy emulyatsiya shaklida yaratiladi. Hujumchi bunday xizmatga ulanadi, lekin u real tizim bilan emas, balki nazorat ostidagi sun’iy muhit bilan ishlayotgan bo‘ladi.

Low-interaction honeypotlarning asosiy afzalligi — ularni o‘rnatish va boshqarish nisbatan oson. Ular kam resurs talab qiladi, xavfsizlik darajasi yuqori bo‘ladi va hujumchiga real tizimga chuqur kirish imkonini bermaydi. Shu sababli bunday honeypotlar ko‘pincha avtomatlashtirilgan hujumlarni, port scanning jarayonlarini, brute-force urinishlarini va oddiy zararli faoliyatni aniqlash uchun ishlatiladi.

Masalan, SSH xizmatiga qaratilgan brute-force hujumlarini kuzatishda low-interaction honeypot foydali bo‘lishi mumkin. Hujumchi SSH serverga ulanayotganini o‘ylaydi va turli login-parollarni sinab ko‘radi. Honeypot esa bu urinishlarni yozib boradi. Natijada qaysi foydalanuvchi nomlari ko‘p ishlatilayotgani, qaysi parollar eng ko‘p sinab ko‘rilayotgani va hujumlar qaysi IP-manzillardan amalga oshirilayotgani aniqlanadi.

Low-interaction honeypotlarning kamchiligi shundaki, ular hujumchining murakkab harakatlarini to‘liq kuzata olmaydi. Chunki bunday honeypotlarda haqiqiy tizim muhiti mavjud emas yoki juda cheklangan bo‘ladi. Tajribali tajovuzkor honeypotning sun’iy ekanligini sezib qolishi mumkin. Shuningdek, zararli dasturlarning tizim ichida qanday ishlashini chuqur tahlil qilish uchun low-interaction honeypot yetarli bo‘lmasligi mumkin.

High-interaction honeypot esa hujumchiga haqiqiy tizimga o‘xshash yoki deyarli to‘liq ishlaydigan muhitni taqdim etadi. Bunda real operatsion tizim, real xizmatlar va haqiqiy dasturiy muhit ishlatilishi mumkin. Tajovuzkor tizimga kirgach, fayllarni ko‘rishi, buyruqlar bajarishi, zararli dastur yuklashi yoki tizimni o‘rganishga harakat qilishi mumkin. Bularning barchasi xavfsizlik mutaxassislari tomonidan kuzatib boriladi.

High-interaction honeypotlarning eng katta afzalligi — hujumchilarning chuqur va real xatti-harakatlarini tahlil qilish imkoniyatidir. Bunday honeypotlar orqali tajovuzkor tizimga kirgandan so‘ng qanday buyruqlarni ishlatishi, qanday fayllarni yuklab olishi, qaysi serverlar bilan bog‘lanishi va qanday zararli faoliyatni amalga oshirishi mumkinligi aniqlanadi. Bu esa kiberxavfsizlik tadqiqotlari uchun juda qimmatli ma’lumot beradi.

Biroq high-interaction honeypotlar xavfsizlik nuqtayi nazaridan ancha ehtiyotkorlikni talab qiladi. Chunki hujumchi bu muhitda ko‘proq erkinlikka ega bo‘ladi. Agar honeypot yetarlicha izolyatsiya qilinmagan bo‘lsa, tajovuzkor undan boshqa tizimlarga hujum qilish uchun foydalanishi mumkin. Shu sababli high-interaction honeypotlar odatda alohida tarmoq segmentida, virtual muhitda yoki qat’iy nazorat ostida joylashtiriladi.

Medium-interaction honeypotlar esa low-interaction va high-interaction honeypotlar o‘rtasidagi oraliq yechim hisoblanadi. Ular hujumchi bilan low-interaction honeypotlarga

qaraganda ko‘proq o‘zaro aloqaga kirishadi, ammo real tizimning to‘liq imkoniyatlarini bermaydi. Bunday honeypotlar xavfsizlik va tahlil chuqurligi o‘rtasida muvozanat yaratadi. Masalan, Cowrie honeypotini SSH va Telnet hujumlarini tahlil qilishda medium-interaction honeypot sifatida ko‘rish mumkin.

Cowrie honeypot SSH va Telnet xizmatlariga qaratilgan hujumlarni o‘rganishda keng qo‘llaniladi. U tajovuzkorga SSH serverga kirgandek ko‘rinadigan muhit yaratadi. Hujumchi login va parol kiritadi, tizimga kirgandek bo‘ladi va buyruqlar bajarishga urinadi. Cowrie esa uning barcha harakatlarini yozib boradi. Masalan, hujumchi ls, pwd, wget, curl, uname, cat /etc/passwd kabi buyruqlarni ishlatsa, honeypot bu buyruqlarni log fayllarga saqlaydi.

Honeypotlar maqsadiga ko‘ra ham bir nechta turlarga bo‘linadi. Masalan, research honeypot va production honeypot tushunchalari mavjud. Research honeypotlar ilmiy tadqiqot va tahlil maqsadida ishlatiladi. Ularning asosiy vazifasi hujumchilar faoliyatini chuqur o‘rganish, yangi zararli dasturlarni aniqlash va hujum metodlarini tahlil qilishdir. Bunday honeypotlar ko‘pincha universitetlar, ilmiy markazlar va kiberxavfsizlik laboratoriyalarida qo‘llaniladi.

Production honeypotlar esa amaliy xavfsizlikni oshirish uchun tashkilotlarning real tarmoqlarida ishlatiladi. Ularning vazifasi tashkilot tarmog‘iga qaratilgan shubhali harakatlarni erta aniqlashdan iborat. Masalan, tashkilot ichki tarmog‘ida hech kim foydalanmaydigan maxsus server joylashtiriladi. Agar kimdir bu serverga ulanishga urinsa, bu darhol shubhali holat sifatida baholanadi. Chunki oddiy foydalanuvchilar bu serverga murojaat qilmasligi kerak.

Honeypotlarning yana bir muhim turi — spam honeypot hisoblanadi. Bunday honeypotlar spam yuboruvchi botlar va zararli email faoliyatini o‘rganish uchun ishlatiladi. Shuningdek, web honeypotlar mavjud bo‘lib, ular veb-ilovalarga qaratilgan hujumlarni aniqlashda qo‘llaniladi. Masalan, SQL injection, XSS, fayl yuklashdagi zaifliklar yoki administrator paneliga kirish urinishlari web honeypot orqali qayd etilishi mumkin.

Malware honeypotlar zararli dasturlarni tutish va tahlil qilish uchun ishlatiladi. Bunday honeypotlar zararli fayllar, botnet aloqalari yoki avtomatik ekspluatatsiya urinishlarini aniqlashga yordam beradi. Database honeypotlar esa ma’lumotlar bazasiga qaratilgan hujumlarni kuzatish uchun ishlatiladi. IoT honeypotlar esa aqlli qurilmalar, kameralar, routerlar va boshqa IoT qurilmalariga qaratilgan hujumlarni o‘rganishda qo‘llaniladi.

Honeypot texnologiyalarining afzalliklari ko‘p. Birinchidan, ular haqiqiy hujumlar haqida amaliy ma’lumot beradi. Oddiy xavfsizlik tizimlari ba’zan noto‘g‘ri ogohlantirishlar berishi mumkin, ammo honeypotga qilingan murojaatning o‘zi odatda shubhali hisoblanadi. Chunki honeypot real foydalanuvchilar uchun mo‘ljallanmagan bo‘ladi. Demak, unga murojaat qilgan subyekt katta ehtimol bilan skaner, bot yoki tajovuzkor bo‘lishi mumkin.

Ikkinchidan, honeypotlar hujumchilarning ishlatadigan login va parollarini aniqlashga yordam beradi. Masalan, SSH honeypot orqali tajovuzkorlar eng ko‘p qaysi foydalanuvchi nomlarini sinab ko‘rayotgani bilib olinadi. Amaliyotda “root”, “admin”, “user”, “test”, “oracle”, “ubuntu” kabi foydalanuvchi nomlari ko‘p uchraydi. Parollar orasida esa “123456”, “password”, “admin”, “root”, “qwerty” kabi zaif variantlar ko‘p sinab ko‘riladi.

Uchinchidan, honeypotlar hujum manbalarini aniqlashga yordam beradi. Log fayllar orqali hujum qilayotgan IP-manzillar, mamlakatlar, vaqt oralig‘i va takroriy urinishlar soni tahlil qilinadi. Bu ma’lumotlar yordamida xavfsizlik siyosatini kuchaytirish, firewall qoidalarini yangilash yoki shubhali IP-manzillarni bloklash mumkin.

To‘rtinchidan, honeypotlar yangi hujum usullarini aniqlash imkonini beradi. Tajovuzkorlar doimiy ravishda yangi skriptlar, avtomatlashtirilgan vositalar va zararli dasturlardan foydalanadilar. Honeypot bu harakatlarni real vaqtga yaqin holatda kuzatib borishi mumkin. Natijada xavfsizlik mutaxassislari yangi tahdidlar haqida erta xabardor bo‘ladilar.

Beshinchidan, honeypotlar kiberxavfsizlik bo‘yicha o‘quv va tajriba muhitini yaratadi. Talabalar, tadqiqotchilar va administratorlar honeypot orqali hujumlar qanday amalga oshirilishini xavfsiz muhitda o‘rganishlari mumkin. Bu esa nazariy bilimlarni amaliy ko‘nikmalar bilan mustahkamlashga yordam beradi.

Shu bilan birga, honeypot texnologiyalarining ayrim kamchiliklari ham mavjud. Birinchidan, honeypotlar noto‘g‘ri sozlansa, tashkilot uchun qo‘shimcha xavf tug‘dirishi mumkin. Ayniqsa high-interaction honeypotlarda hujumchi tizimdan boshqa tarmoqlarga hujum qilish uchun foydalanishi ehtimoli bor. Shu sababli honeypotlar izolyatsiya qilingan muhitda ishlashi kerak.

Ikkinchidan, honeypotlarni muntazam kuzatish va tahlil qilish talab etiladi. Faqat honeypotni o‘rnatishning o‘zi yetarli emas. Undan olingan loglar, statistikalar va hujum izlari muntazam ravishda ko‘rib chiqilishi kerak. Aks holda, honeypot foydali ma’lumot yig‘sa ham, bu ma’lumotlar xavfsizlik choralariga aylantirilmaydi.

Uchinchidan, tajribali hujumchilar honeypotni aniqlashi mumkin. Agar honeypot haqiqiy tizimga yetarlicha o‘xshamasa, tajovuzkor uning sun’iy ekanligini sezib qoladi va faoliyatini to‘xtatadi. Masalan, buyruqlarning noto‘g‘ri ishlashi, fayl tizimining juda sodda bo‘lishi yoki tizim javoblarining real serverga o‘xshamasligi honeypotni fosh qilishi mumkin.

To‘rtinchidan, honeypotlar barcha hujumlarni aniqlay olmaydi. Ular faqat o‘zlariga yo‘naltirilgan yoki ularning xizmatlariga tegishli bo‘lgan faoliyatni qayd etadi. Masalan, SSH honeypot veb-ilovalarga qaratilgan SQL injection hujumlarini to‘liq ko‘rsatib bera olmaydi. Shuning uchun honeypotlar boshqa xavfsizlik vositalari bilan birgalikda ishlatilishi kerak.

Honeypot texnologiyalari hujumchilar faoliyatini kuzatishda muhim rol o‘ynaydi. Ular orqali hujumning boshlanish bosqichidan tortib, tizimga kirish urinishlari va keyingi harakatlargacha bo‘lgan jarayonni o‘rganish mumkin. Masalan, SSH honeypotda dastlab port scanning qayd etiladi. Keyin tajovuzkor login-parollarni sinab ko‘radi. Agar honeypot unga tizimga kirgandek imkon bersa, keyingi bosqichda hujumchi buyruqlar bajarishga, tizim haqida ma’lumot yig‘ishga yoki zararli fayllarni yuklab olishga urinadi. Bu jarayonni kuzatish kiberxavfsizlik mutaxassislariga hujum zanjirini tushunishga yordam beradi. Hujum zanjiri deganda tajovuzkorning nishonni aniqlash, zaiflikni topish, kirish, tizimda mustahkamlanish, ma’lumot yig‘ish va zararli faoliyatni davom ettirish bosqichlari tushuniladi. Honeypot aynan shu bosqichlarni amaliy ko‘rinishda tahlil qilish imkonini beradi.

Honeypotlardan olingan ma’lumotlar xavfsizlik monitoringi tizimlariga ham integratsiya qilinishi mumkin. Masalan, honeypot loglari SIEM tizimlariga yuboriladi. SIEM tizimi esa bu

loglarni boshqa manbalardan kelayotgan ma’lumotlar bilan solishtirib, umumiy xavfsizlik holatini tahlil qiladi. Agar honeypotda biror IP-manzildan hujum qayd etilsa va shu IP keyinchalik real serverga ham murojaat qilsa, bu jiddiy xavf sifatida baholanishi mumkin.

Honeypotlar IDS va IPS tizimlari bilan ham birgalikda ishlatiladi. IDS hujumni aniqlash tizimi bo‘lsa, IPS hujumni oldini olish tizimi hisoblanadi. Honeypot esa ularga qo‘shimcha ma’lumot manbai bo‘lib xizmat qiladi. Masalan, honeypot orqali aniqlangan zararli IP-manzillar firewall yoki IPS qoidalariga qo‘shilishi mumkin. Bu orqali real tizimlarga qaratilgan hujumlar kamaytiriladi.

SSH xizmatiga qaratilgan hujumlarni o‘rganishda honeypotlar ayniqsa muhimdir. Chunki internetda ochiq SSH xizmatlari juda ko‘p hujumlarga duch keladi. Tajovuzkorlar avtomatlashtirilgan botlar yordamida 22-portni skanerlaydi, keyin esa brute-force yoki dictionary attack usullarini qo‘llaydi. Cowrie kabi SSH honeypotlar bu jarayonni to‘liq kuzatib, hujumchilarning login-parol bazasi va buyruqlar ketma-ketligini aniqlashga yordam beradi. Masalan, SSH honeypotga kirgan tajovuzkor tizim haqida ma’lumot olish uchun uname -a, whoami, id, ifconfig, ip addr, cat /proc/cpuinfo kabi buyruqlarni bajarishi mumkin. Ba’zi holatlarda u zararli skriptni yuklab olish uchun wget yoki curl buyruqlaridan foydalanadi. Bu buyruqlar orqali tajovuzkor serverni botnetga qo‘shish, kriptovalyuta qazish dasturini o‘rnatish yoki boshqa zararli harakatlarni amalga oshirishga urinishi mumkin. Honeypot esa bu buyruqlarning barchasini qayd etadi.

Honeypotlardan foydalanish tashkilot xavfsizlik siyosatini takomillashtirishga ham yordam beradi. Masalan, honeypot loglarida “root” foydalanuvchisiga juda ko‘p hujum bo‘layotgani ko‘rinsa, real serverlarda root orqali SSH kirishini taqiqlash zarurligi yanada yaqqol namoyon bo‘ladi. Agar zaif parollar ko‘p sinab ko‘rilayotgani aniqlansa, kuchli parol siyosatini joriy etish va parol orqali kirishni cheklash maqsadga muvofiq bo‘ladi.

Honeypot texnologiyalari kiberxavfsizlikda faqat mudofaa vositasi emas, balki tahliliy vosita sifatida ham muhimdir. Ular real hujumlarni chuqur o‘rganish, hujumchilar psixologiyasi va texnikasini tushunish, xavfsizlik zaifliklarini aniqlash va yangi himoya strategiyalarini ishlab chiqishga yordam beradi. Shu sababli honeypotlar kiberxavfsizlik tadqiqotlarida, universitet laboratoriyalarida, xavfsizlik operatsion markazlarida va amaliy tarmoq himoyasida keng qo‘llaniladi.

Umuman olganda, honeypot texnologiyalari zamonaviy kiberxavfsizlik tizimining muhim tarkibiy qismi hisoblanadi. Ular hujumchilarni chalg‘itish, ularning faoliyatini kuzatish, hujum usullarini tahlil qilish va real tizimlarni himoya qilishda qo‘shimcha imkoniyat yaratadi. Low-interaction honeypotlar oddiy va xavfsiz bo‘lsa, high-interaction honeypotlar chuqur tahlil imkonini beradi. Har ikkala tur ham o‘z o‘rnida foydali bo‘lib, to‘g‘ri qo‘llanilganda tashkilotning umumiy xavfsizlik darajasini oshiradi. Shu sababli “Cowrie honeypot asosida SSH xizmatiga qilingan hujumlarni monitoring va tahlil qilish” mavzusidagi diplom loyiha ishida honeypot texnologiyalarini o‘rganish muhim nazariy asos bo‘lib xizmat qiladi. Honeypot yordamida SSH hujumlarini amaliy kuzatish, tajovuzkorlarning login-parol urinishlarini tahlil qilish, ularning buyruqlarini o‘rganish va real serverlar uchun samarali himoya choralarini ishlab chiqish mumkin. Demak, honeypot texnologiyalari kiberxavfsizlikda nafaqat hujumlarni aniqlash, balki ularni chuqur tushunish va oldini olishda ham katta ahamiyatga ega.

1.1-jadval

Honeypot texnologiyasining zamonaviy kiberxavfsizlik texnologiyalari bilan tahlili

Taqqoslash mezoni	**Honeypot**	**Firewall**	**IDS/IPS**	**SIEM**
Asosiy vazifasi	Tajovuzkorni aldamchi tizimga jalb qilish va hujum usullarini o‘rganish	Tarmoq trafikini ruxsat berilgan/qaytarilgan qoidalarga ko‘ra boshqarish	Hujumni aniqlash va ayrim hollarda to‘xtatish	Turli manbalardan loglarni yig‘ish va tahlil qilish
Himoya turi	Aldash va tahlil qilishga asoslangan	Oldini olishga asoslangan	Aniqlash va bloklashga asoslangan	Monitoring va tahlilga asoslangan
Hujumni aniqlash darajasi	Yuqori, chunki honeypotga kirishning o‘zi shubhali hisoblanadi	O‘rtacha, qoidalar to‘g‘ri sozlansa samarali	Yuqori, real vaqtga yaqin ogohlantirish beradi	Yuqori, ko‘p manbali loglarni bog‘laydi
SSH hujumlariga mosligi	Juda mos: brute-force, dictionary attack, credential stuffing urinishlarini yozib boradi	SSH portini cheklash yoki bloklashda foydali	SSH trafikidagi shubhali urinishlarni aniqlaydi	SSH loglarini markazlashgan holda tahlil qiladi
Ma’lumot yig‘ish imkoniyati	Juda kuchli: tajovuzkor IP manzili,	Cheklangan: asosan trafik va bloklangan	O‘rtacha/yaxshi: hodisa va ogohlantirishlar	Juda kuchli: loglar, hodisalar, korrelyatsiya

	parollar, buyruqlar va usullarni yozadi	ulanishlar	ni beradi	
Real tizimga ta'siri	To‘g‘ri ajratilsa, real tizimga xavf kamayadi	Real tizimni bevosita himoya qiladi	Real trafikni kuzatadi yoki bloklaydi	Real tizim loglari asosida ishlaydi
Afzalligi	Hujumchini chalg‘itadi, yangi hujum usullarini o‘rganishga yordam beradi	Oddiy va zaruriy birinchi himoya qatlami	Hujumlarni tez aniqlash imkonini beradi	Katta tizimlarda markaziy nazorat beradi
Kamchiligi	Noto‘g‘ri sozlansa, tajovuzkor undan foydalanib qolishi mumkin	Faqat qoidalar asosida ishlaydi, murakkab hujumlarni o‘zi tahlil qilmaydi	False positive ko‘p bo‘lishi mumkin	Sozlash va tahlil qilish murakkab

Ushbu jadvalda honeypot texnologiyasi hozirgi kunda keng qo‘llaniladigan firewall, IDS/IPS va SIEM kabi kiberxavfsizlik texnologiyalari bilan taqqoslandi. Taqqoslash 8 ta asosiy mezon asosida amalga oshirildi: asosiy vazifasi, himoya turi, hujumlarni aniqlash darajasi, SSH hujumlariga mosligi, ma'lumot yig‘ish imkoniyati, real tizimga ta'siri, afzalligi va kamchiligi.

Jadvaldan ko‘rinib turibdiki, firewall asosan tarmoq trafikini nazorat qilish va ruxsatsiz ulanishlarni cheklash uchun xizmat qiladi. IDS/IPS texnologiyalari esa tizimdagi shubhali harakatlarni aniqlash va ayrim hollarda ularni avtomatik bloklash imkonini beradi. SIEM tizimlari turli manbalardan kelgan loglarni yig‘ib, ularni markazlashgan holda tahlil qiladi. EDR/XDR texnologiyalari endpoint qurilmalarda yuz berayotgan tahdidlarni chuqurroq kuzatadi. WAF asosan veb-ilovalarni himoya qilishga qaratilgan bo‘lsa, SOAR xavfsizlik hodisalariga avtomatik javob qaytarish jarayonini tezlashtiradi.

Honeypot texnologiyasining asosiy farqi shundaki, u hujumni faqat bloklash yoki aniqlash bilan cheklanmaydi. U tajovuzkorni maxsus tayyorlangan aldamchi tizimga jalb qiladi va uning harakatlarini kuzatadi. Masalan, SSH xizmatiga qaratilgan brute-force, dictionary attack yoki credential stuffing hujumlarida honeypot tajovuzkor kiritgan login-parollarni, IP manzillarni, ulanish vaqtini va bajarilgan buyruqlarni yozib borishi mumkin. Shu sababli honeypot texnologiyasi ilmiy va amaliy jihatdan juda foydali hisoblanadi. U orqali tashkilotlar real hujum usullarini o‘rganishi, zaif parollar ro‘yxatini aniqlashi, tajovuzkorlarning ishlash uslubini tahlil qilishi va keyinchalik himoya choralarini kuchaytirishi mumkin. Ayniqsa, Cowrie kabi SSH

honeypotlar SSH xizmatlariga bo‘ladigan hujumlarni monitoring qilish va tahlil qilishda samarali vosita hisoblanadi.

Honeypot texnologiyasi boshqa himoya vositalarining o‘rnini to‘liq bosa olmaydi, lekin ularni to‘ldiruvchi muhim xavfsizlik mexanizmi hisoblanadi. Firewall, IDS/IPS va SIEM kabi vositalar tizimni himoya qilishga xizmat qilsa, honeypot tajovuzkorning harakatlarini o‘rganish, hujum ssenariylarini aniqlash va xavfsizlik choralarini takomillashtirish imkonini beradi.

Xulosa

Tadqiqot natijalari shuni ko‘rsatdiki, honeypot texnologiyalari zamonaviy kiberxavfsizlik tizimlarining muhim tarkibiy qismlaridan biri hisoblanadi. Ular real axborot resurslariga zarar yetkazmasdan turib hujumchilarning harakatlarini kuzatish, hujum usullarini tahlil qilish va yangi tahdidlarni erta aniqlash imkonini beradi. Honeypotlardan foydalanish natijasida tarmoq infratuzilmasidagi zaifliklarni aniqlash, zararli dasturlar faoliyatini o‘rganish hamda axborot tizimlarining himoyalanganlik darajasini oshirish mumkin.

Ayniqsa, honeypot texnologiyalarini IDS, IPS, SIEM va boshqa xavfsizlik vositalari bilan integratsiya qilish kiberhujumlarni aniqlash samaradorligini sezilarli darajada oshiradi. Kelgusida sun'iy intellekt va mashinali o‘qitish texnologiyalarini honeypot tizimlariga tatbiq etish avtomatik tahlil va tahdidlarni prognoz qilish imkoniyatlarini yanada kengaytiradi. Shu sababli, honeypot texnologiyalarini davlat tashkilotlari, korxonalar va ta'lim muassasalarining axborot tizimlarida qo‘llash kiberxavfsizlikni ta'minlashning samarali yo‘nalishlaridan biri hisoblanadi.

Foydalanilgan adabiyotlar

1. Spitzner L. *Honeypots: Tracking Hackers*. Addison-Wesley, 2003.
2. Provos N., Holz T. *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Addison-Wesley, 2008.
3. NIST. *Guide to Intrusion Detection and Prevention Systems (SP 800-94)*. National Institute of Standards and Technology, 2007.
4. ENISA. *Threat Landscape Report*. European Union Agency for Cybersecurity, 2024.
5. Scarfone K., Mell P. *Guide to Intrusion Detection and Prevention Systems*. NIST Special Publication 800-94, 2007.
6. Stallings W. *Network Security Essentials: Applications and Standards*. Pearson, 2023.
7. Anderson R. *Security Engineering*. 3rd Edition. Wiley, 2020.
8. OWASP Foundation. *OWASP Top 10: The Ten Most Critical Web Application Security Risks*. 2021.
9. CISA. *Cybersecurity Best Practices*. 2024.
10. RFC 4949. *Internet Security Glossary, Version 2*. IETF, 2007.