INTERNATIONAL JOURNAL OF TECHNOLOGY AND ACADEMIC RESEARCH

ISSN: 2224-6878 | Pakistan Volume 6, No. 8.

IF: 15.9 | 2026 http://waerasia.org/index.php/ijtar

COWRIE HONEYPOT INSTALLATION, CONFIGURATION AND SSH ATTACK LOGGING PROCESS

Khorozov Khumoyun Inomjon oglu,

Mamatkarimov Asadbek Anvarjonovich,

Qaxramonov Sardor,

Sotvoldiyev Asadbek

Students of TUIT, Cybersecurity faculty

Doi: https://doi.org/10.5281/zenodo.21757903

Abstract: This article covers the process of installing the Cowrie honeypot system on the Linux operating system, initial configuration, and recording of cyberattacks targeting the SSH service. In the course of the study, the architecture, configuration files, as well as log-entry generation mechanisms of the Cowrie software were analyzed. It also looked at the ways in which log data can be collected, analyzed, and used to ensure cybersecurity as a result of brute force and dictionary attacks. The results obtained showed that the Cowrie honeypot system is an effective tool for early detection and analysis of attacks on real-world networks.

Keywords: Cowrie honeypot, SSH, Telnet, OpenSSH, cybersecurity, honeypot, Linux, log files, threat detection.

COWRIE HONEYPOTNI O‘RNATISH, SOZLASH VA SSH HUJUMLARINI QAYD ETISH JARAYONI

Annotatsiya: Mazkur maqolada Cowrie honeypot tizimini Linux operatsion tizimiga o‘rnatish, dastlabki sozlash va SSH xizmatiga qaratilgan kiberhujumlarni qayd etish jarayoni yoritilgan. Tadqiqot davomida Cowrie dasturiy ta'minotining arxitekturasi, konfiguratsiya fayllari hamda log yozuvlarini shakllantirish mexanizmlari tahlil qilindi. Shuningdek, brute force va lug‘at (dictionary) hujumlari natijasida hosil bo‘ladigan jurnal ma'lumotlarini yig‘ish, tahlil qilish va ulardan kiberxavfsizlikni ta'minlashda foydalanish usullari ko‘rib chiqildi. Olingan natijalar Cowrie honeypot tizimi real tarmoqlarda hujumlarni erta aniqlash va tahlil qilishda samarali vosita ekanligini ko‘rsatdi.

Kalit so‘zlar: Cowrie honeypot, SSH, Telnet, OpenSSH, kiberxavfsizlik, honeypot, Linux, hujumlarni monitoring qilish, log fayllari, tahdidlarni aniqlash.

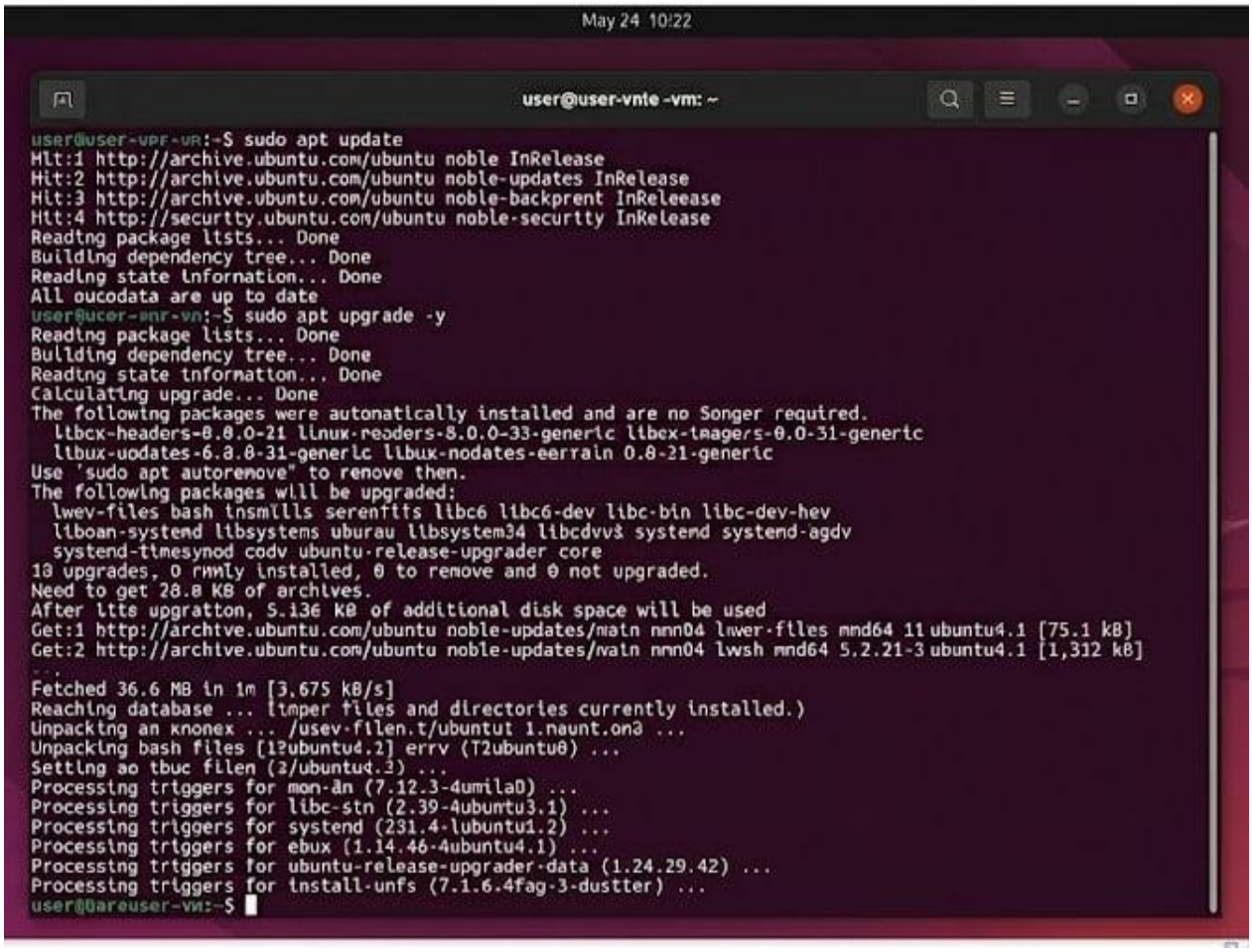
Cowrie honeypot SSH va Telnet xizmatlariga qaratilgan hujumlarni kuzatish, qayd etish va tahlil qilish uchun mo‘ljallangan maxsus dasturiy vosita hisoblanadi. Ushbu diplom loyiha ishida Cowrie honeypotdan SSH xizmatiga bo‘ladigan brute-force, dictionary attack, credential stuffing va ruxsatsiz kirish urinishlarini monitoring qilish maqsadida foydalaniladi. Cowrie orqali hujumchilarning IP-manzillari, login-parol urinishlari, terminalda bajargan buyruqlari va sessiya ma’lumotlari log fayllarga yozib boriladi.

ISSN: 2224-6878 | Pakistan Volume 6, No. 8.

IF: 15.9 | 2026 http://waerasia.org/index.php/ijtar

Cowrie honeypotni o‘rnatish jarayoni Linux muhitida amalga oshiriladi. Buning uchun Ubuntu Server yoki Debian operatsion tizimidan foydalanish mumkin. Honeypotni asosiy ishchi serverga emas, balki alohida virtual mashinaga o‘rnatish maqsadga muvofiqdir. Chunki honeypot ataylab hujumchilarni o‘ziga jalb qiluvchi tizim bo‘lib, uni real serverlardan ajratilgan holda ishlatish xavfsizlik talablariga mos keladi.

Birinchi bosqichda Cowrie honeypot uchun alohida Linux virtual mashinasi tayyorlanadi. Bunda VirtualBox, VMware yoki Proxmox kabi virtualizatsiya vositalaridan foydalanish mumkin. Virtual mashinaga Ubuntu Server yoki Debian o‘rnatiladi. Tizimga internet ulanishi beriladi, chunki kerakli paketlar va kutubxonalar internet orqali yuklab olinadi.



1.1-rasm. Cowrie honeypot uchun Linux virtual mashinasini tayyorlash

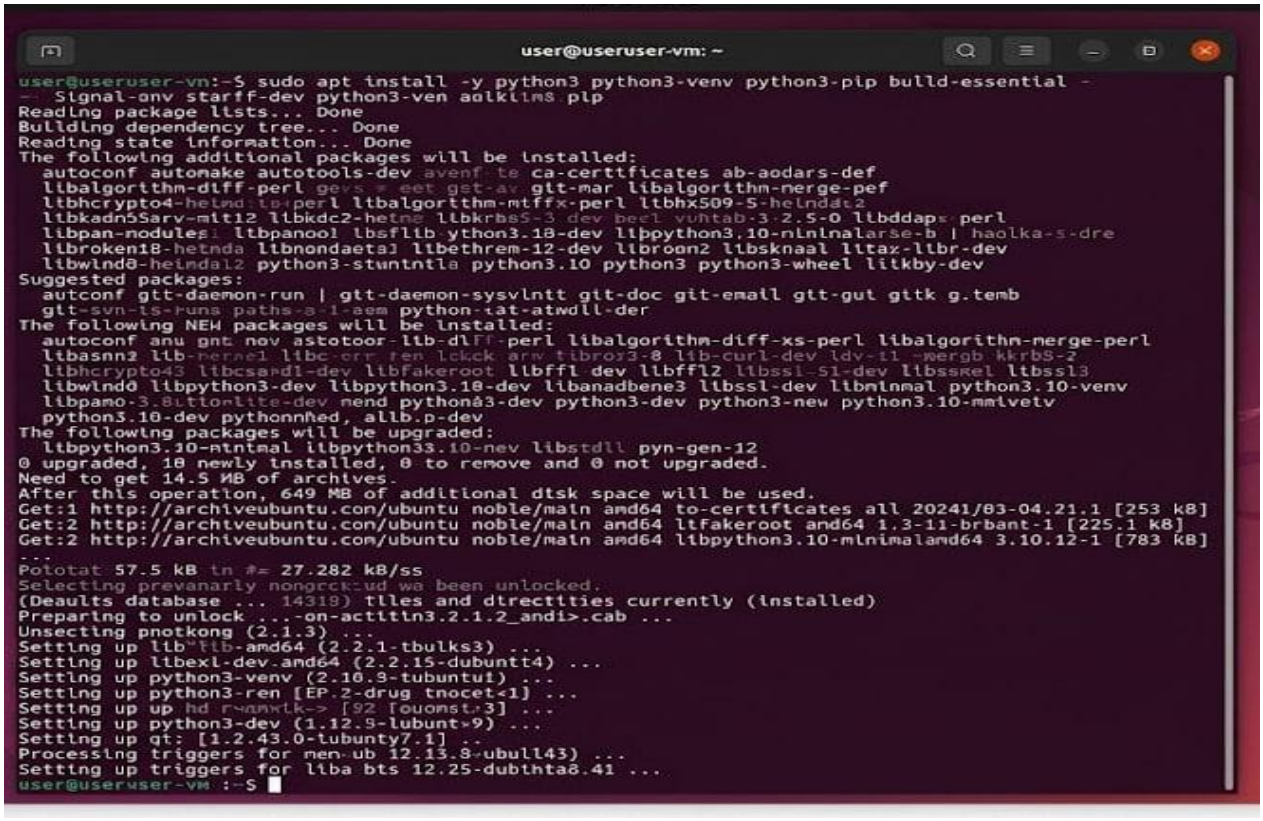
Cowrie honeypotni xavfsiz ishlatish uchun alohida Linux virtual mashinasi yaratildi. Bu usul honeypotni asosiy tizimdan ajratib, hujumlarni nazorat ostida kuzatish imkonini beradi. sudo apt update, sudo apt upgrade -y, ushbu buyruqlar Linux tizimini yangilash va xavfsizlik yamoqlarini o‘rnatish uchun ishlatiladi. Yangilangan tizimda Cowrie honeypotni o‘rnatish ancha barqaror va xavfsiz amalga oshiriladi.

Cowrie Python dasturlash tili asosida ishlaydi. Shu sababli tizimga Python, pip, virtual environment va boshqa kerakli kutubxonalar o‘rnatiladi. Terminalda quyidagi buyruq bajariladi: sudo apt install -y python3 python3-venv python3-pip build-essential libssl-dev libffi-dev python3-dev authbind git. Bu buyruq Cowrie ishlashi uchun zarur bo‘lgan asosiy paketlarni o‘rnatadi. python3 Cowrie dasturini ishga tushirish uchun, python3-venv virtual muhit yaratish

ISSN: 2224-6878 | Pakistan Volume 6, No. 8.

IF: 15.9 | 2026 http://waerasia.org/index.php/ijtar

uchun, python3-pip esa Python paketlarini o‘rnatish uchun kerak bo‘ladi. authbind esa past portlar bilan ishlashda foydali bo‘lishi mumkin.



1.2-rasm. Linux tizimida kerakli paketlarni o‘rnatish

Cowrie honeypot ishlashi uchun Python, pip, virtual muhit va zarur kutubxonalar Linux tizimiga o‘rnatildi. Bu bosqichdan so‘ng tizim Cowrie honeypotni o‘rnatishga tayyor holatga keladi.

Cowrie honeypotni root foydalanuvchisi nomidan ishga tushirish xavfsiz emas. Shuning uchun Cowrie uchun alohida foydalanuvchi yaratiladi. Bu foydalanuvchi cheklangan huquqlarga ega bo‘ladi va honeypot jarayonlari shu foydalanuvchi nomidan bajariladi.

Terminalda quyidagi buyruq yoziladi: sudo adduser --disabled-password cowrie. Bu buyruq cowrie nomli foydalanuvchini yaratadi. Keyin ushbu foydalanuvchiga o‘tiladi: sudo su – cowrie. Endi keyingi barcha Cowrie bilan bog‘liq amallar cowrie foydalanuvchisi nomidan bajariladi. Bu usul xavfsizlikni oshiradi, chunki honeypotda biror xavfli holat yuzaga kelsa ham, u butun tizimga yuqori huquqlar bilan ta’sir qila olmaydi.

ISSN: 2224-6878 | Pakistan Volume 6, No. 8.

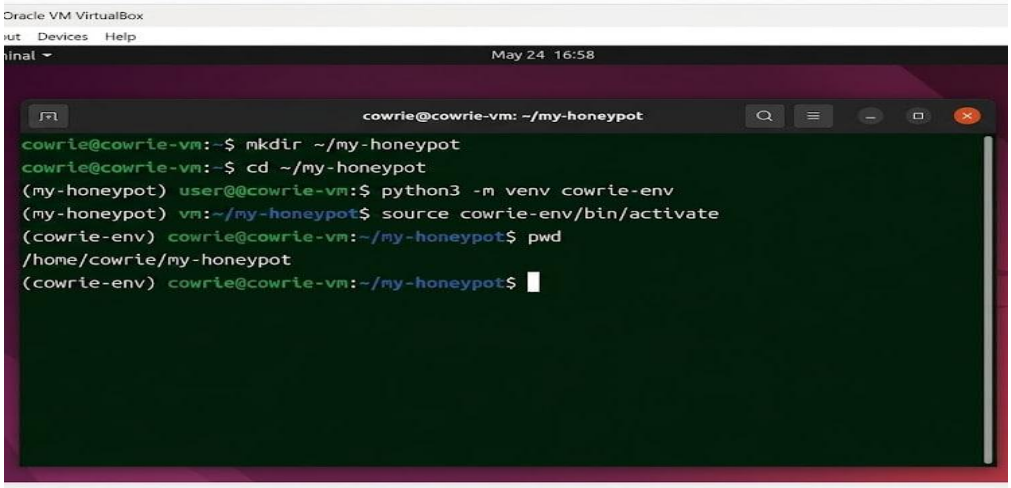
IF: 15.9 | 2026 http://waerasia.org/index.php/ijtar



1.3-rasm. Cowrie uchun alohida foydalanuvchi yaratish

Cowrie honeypot root huquqlari bilan emas, alohida cowrie foydalanuvchisi nomidan ishga tushiriladi. Bu tizim xavfsizligini oshiradi.

Cowrie'ni asosiy tizim kutubxonalaridan ajratib o'rnatish uchun Python virtual muhiti yaratiladi. Virtual muhit dastur uchun alohida kutubxonalar to'plamini shakllantiradi va boshqa tizim paketlariga ta'sir qilmaydi. Agar terminal satrida (cowrie-env) yozuvi paydo bo'lsa, virtual muhit muvaffaqiyatli faollashgan bo'ladi. Endi Cowrie va unga kerakli Python kutubxonalari aynan shu virtual muhitga o'rnatiladi.



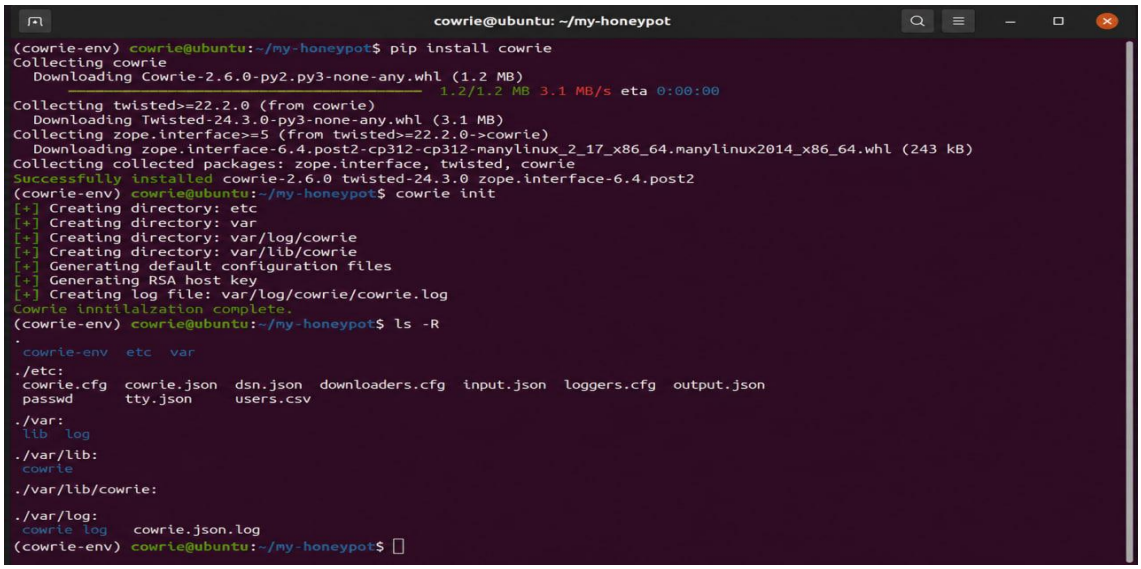
1.4-rasm. Python virtual muhitini yaratish va faollashtirish

Cowrie honeypot uchun alohida Python virtual muhiti yaratildi. Bu muhit Cowrie kutubxonalarini asosiy tizim kutubxonalaridan ajratib turadi.

Virtual muhit faollashtirilgandan so'ng Cowrie honeypot pip orqali o'rnatiladi: pip install cowrie. Ushbu buyruq Cowrie dasturini va unga bog'liq Python kutubxonalarini yuklab olib o'rnatadi. O'rnatish tugagandan so'ng Cowrie uchun boshlang'ich katalog va fayllar yaratiladi. etc katalogida Cowrie konfiguratsiya fayllari joylashadi. var/log/cowrie katalogida esa SSH va Telnet hujumlariga oid log fayllar saqlanadi.

ISSN: 2224-6878 | Pakistan Volume 6, No. 8.

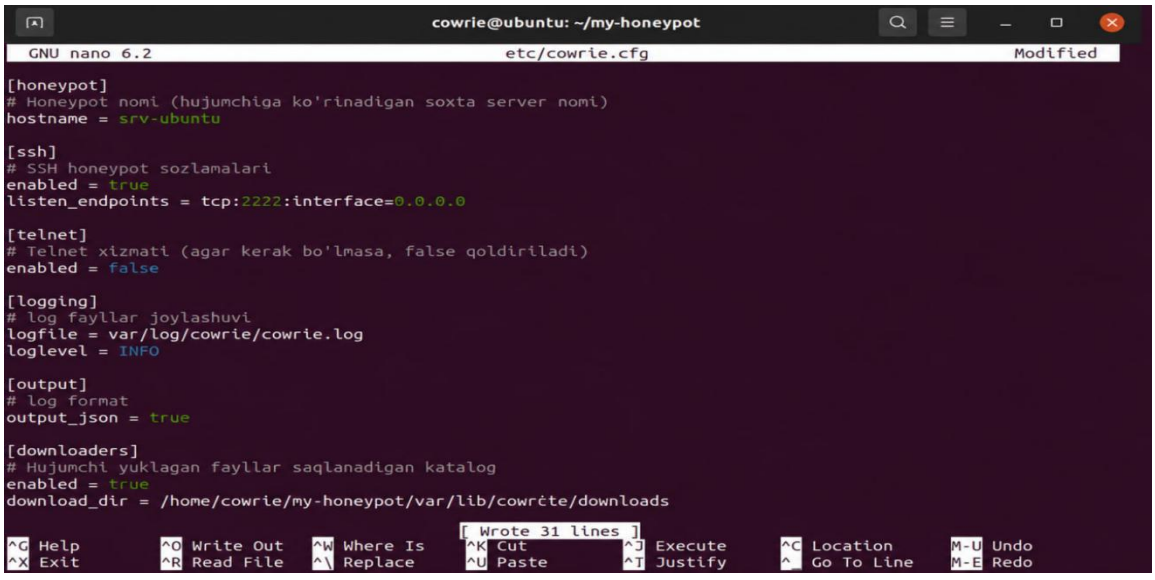
IF: 15.9 | 2026 http://waerasia.org/index.php/ijtar



1.5-rasm. Cowrie honeypotni o‘rnatish va boshlang‘ich kataloglarni yaratish

pip install cowrie buyrug‘i orqali Cowrie o‘rnatildi, cowrie init buyrug‘i yordamida esa konfiguratsiya va log kataloglari yaratildi.

Cowrie honeypotning asosiy sozlamalari cowrie.cfg faylida saqlanadi. Ushbu fayl orqali honeypot nomi, SSH porti, Telnet holati va loglash sozlamalari belgilanadi. Keyin SSH xizmati yoqiladi va Cowrie ishlaydigan port belgilanadi. Bu sozlama Cowrie’ning 2222-portda SSH honeypot sifatida ishlashini bildiradi. Agar Telnet hujumlari ham kuzatilmasa, Telnet xizmatini o‘chirib qo‘yish mumkin. Konfiguratsiya fayli sozlangandan so‘ng fayl saqlanadi va terminalga qaytiladi.



1.6-rasm. Cowrie konfiguratsiya faylini sozlash

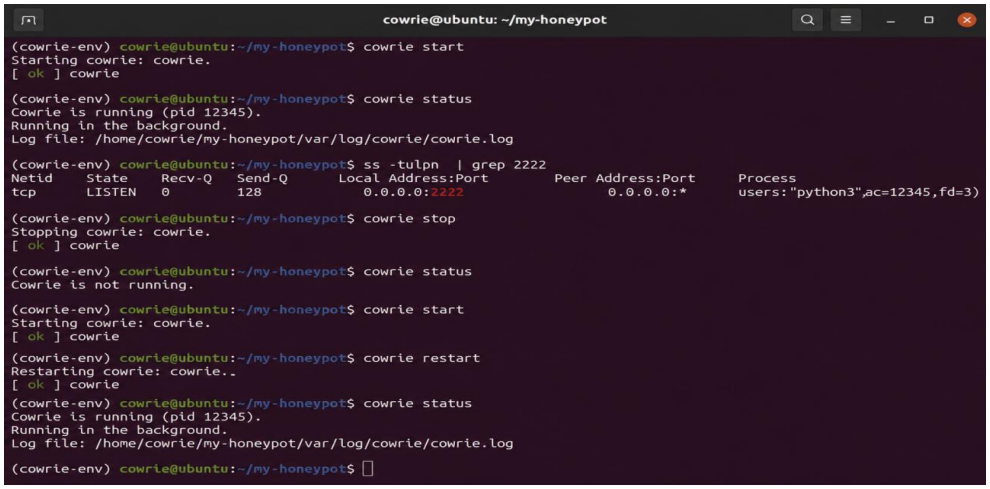
cowrie.cfg faylida honeypot nomi, SSH porti va Telnet xizmati holati sozlandi. Ushbu sozlamalar Cowrie’ning qanday xizmatlarni taqlid qilishini belgilaydi.

Konfiguratsiya sozlangandan so‘ng Cowrie honeypot ishga tushiriladi. Agar Cowrie muvaffaqiyatli ishga tushgan bo‘lsa, uning faol holatda ekanligi ko‘rinadi. Cowrie ishlayotgan

ISSN: 2224-6878 | Pakistan Volume 6, No. 8.

IF: 15.9 | 2026 http://waerasia.org/index.php/ijtar

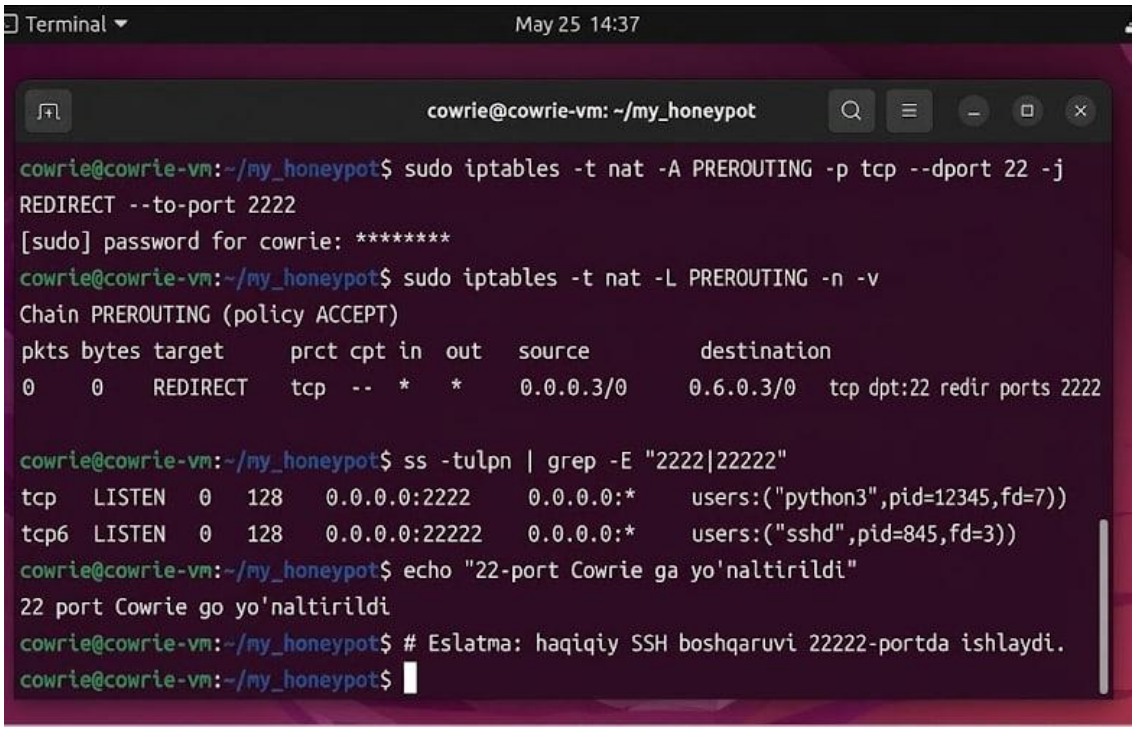
portni tekshirish uchun quyidagi buyruq bajariladi. Agar natijada 2222-port ko‘rinsa, demak Cowrie SSH ulanishlarini qabul qilishga tayyor.



1.7-rasm. Cowrie honeypotni ishga tushirish va holatini tekshirish

cowrie start buyrug‘i orqali hon Cowrie odatda 2222-portda ishlaydi. Biroq haqiqiy SSH xizmati odatda 22-port orqali ishlaydi. Tajovuzkorlar ham ko‘pincha aynan 22-portni skanerlaydi. Shu sababli tashqi 22-portga kelgan SSH ulanishlarini Cowrie ishlayotgan 2222-portga yo‘naltirish mumkin. Bu qoida tashqi tomondan 22-portga kelgan ulanishlarni 2222-portga yo‘naltiradi. Natijada tajovuzkor serverning oddiy SSH xizmatiga ulanayotganini o‘ylaydi, aslida esa Cowrie honeypotga ulanadi.

Agar administrator serverga SSH orqali ulanib ishlayotgan bo‘lsa, bu bosqichda ehtiyot bo‘lish kerak. Chunki 22-port Cowrie’ga yo‘naltirilsa, haqiqiy SSH boshqaruv kanali yopilib qolishi mumkin. Shuning uchun haqiqiy SSH xizmatini oldindan boshqa portga, masalan, 22222-portga ko‘chirish tavsiya etiladi.



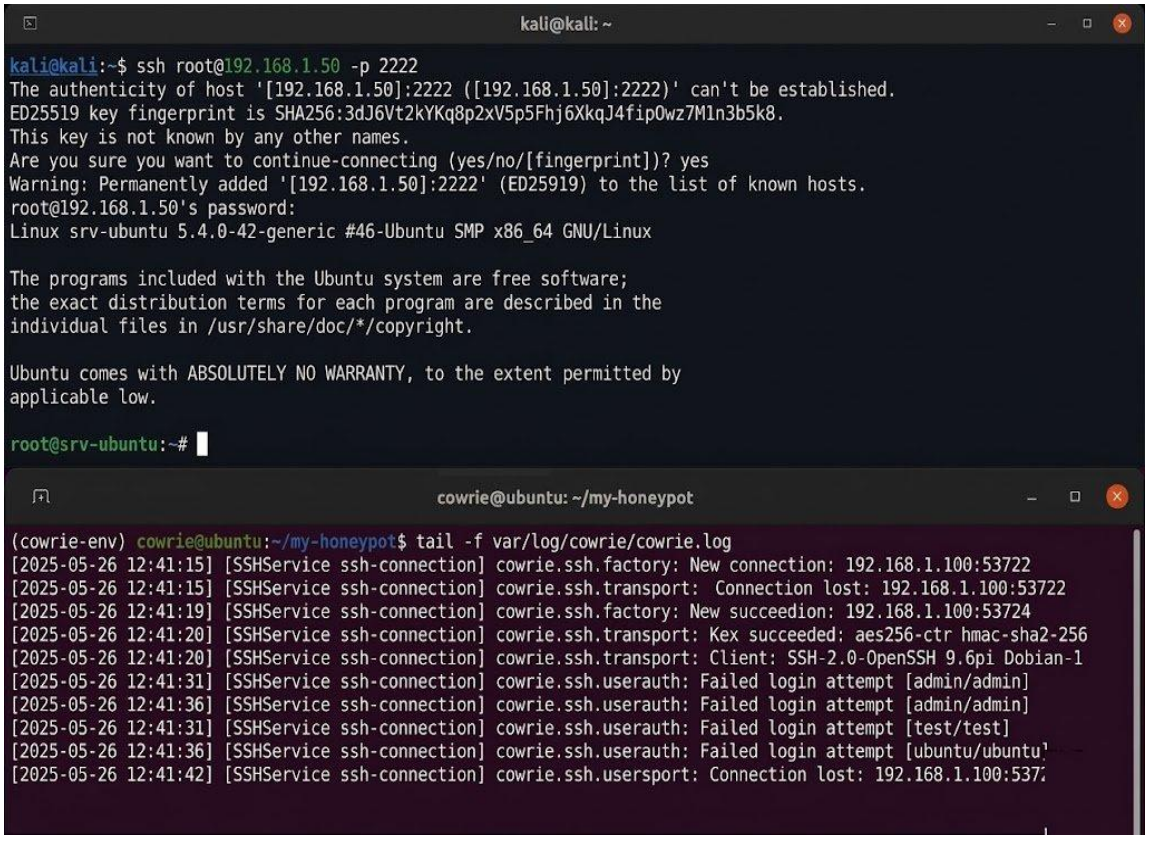
ISSN: 2224-6878 | Pakistan Volume 6, No. 8.

IF: 15.9 | 2026 http://waerasia.org/index.php/ijtar

1.8-rasm. SSH portini Cowrie portiga yo‘naltirish

Tashqi 22-portga kelgan SSH ulanishlari Cowrie ishlayotgan 2222-portga yo‘naltirildi. Bu usul Cowrie’ni tashqi foydalanuvchilar uchun oddiy SSH server sifatida ko‘rsatadi. eypot ishga tushirildi, cowrie status orqali esa uning faol holatda ekanligi tekshirildi.

Cowrie to‘g‘ri ishlayotganini tekshirish uchun boshqa terminal yoki boshqa kompyuterdan SSH orqali test ulanish amalga oshiriladi. Bu yerda SERVER_IP o‘rniga Cowrie o‘rnatilgan serverning IP-manzili yoziladi. Masalan: Test vaqtida istalgan login va parol kiritiladi. Cowrie bu urinishlarni log fayllarga yozib boradi. Masalan, root, admin, test, ubuntu kabi foydalanuvchi nomlari va oddiy parollar sinab ko‘rilsa, ular Cowrie loglarida aks etadi.



1.9-rasm. Cowrie honeypotga SSH orqali test ulanish

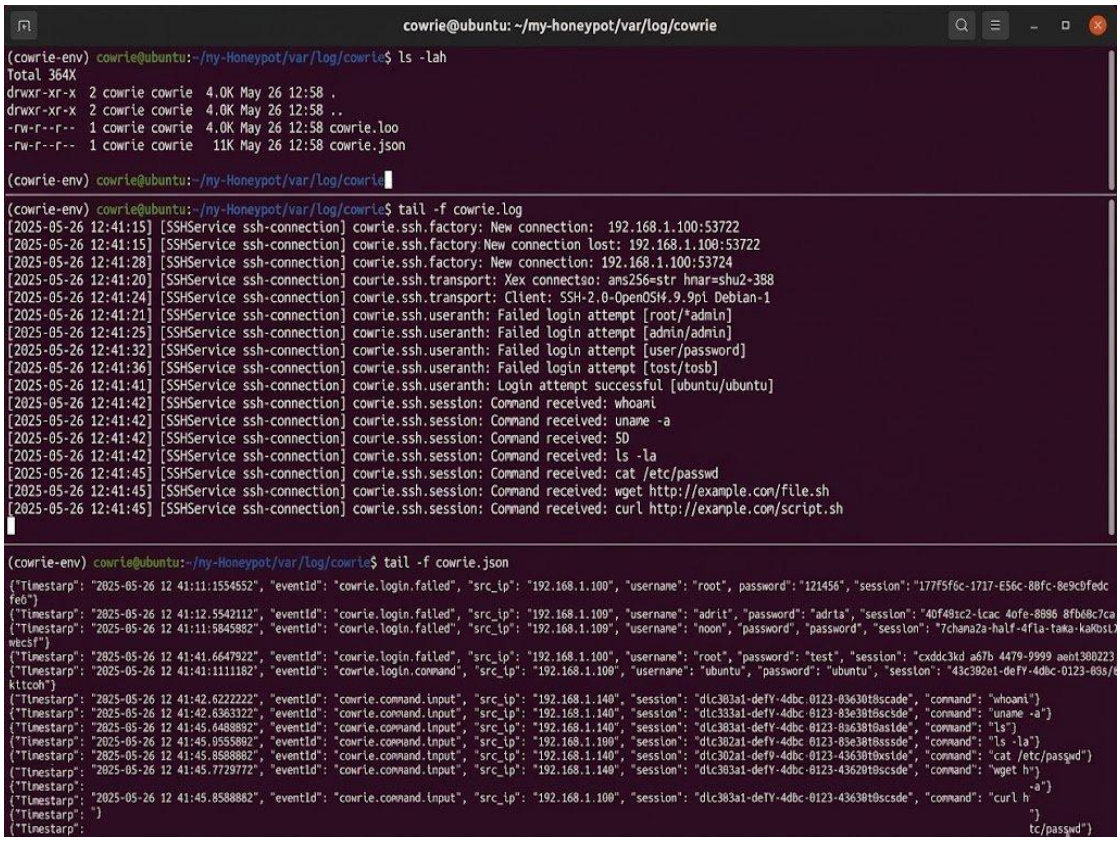
SSH orqali test ulanish amalga oshirildi. Kiritilgan login va parol urinishlari Cowrie log fayllariga yozilishi tekshirildi.

Cowrie honeypotning asosiy natijasi log fayllarda saqlanadi. Log fayllar quyidagi katalogda joylashadi. Masalan, hujumchi quyidagi login-parol kombinatsiyalarini sinab ko‘rishi mumkin. Cowrie bularni log fayllarga yozib boradi. Keyinchalik bu ma’lumotlar asosida eng ko‘p ishlatilgan loginlar va zaif parollar aniqlanadi.

Agar hujumchi soxta terminalga kirsa, u quyidagi buyruqlarni bajarishga urinishi mumkin. Cowrie ushbu buyruqlarni ham saqlab boradi. Bu esa hujumchining tizimda nima qilmoqchi bo‘lganini tahlil qilish imkonini beradi.

ISSN: 2224-6878 | Pakistan Volume 6, No. 8.

IF: 15.9 | 2026 http://waerasia.org/index.php/ijtar



1.10-rasm. Cowrie log fayllarida SSH hujumlarini kuzatish

Cowrie log fayllarida SSH ulanishlari, login-parol urinishlari, hujumchi IP-manzillari va terminal buyruqlari qayd etildi. Ushbu loglar keyinchalik statistik va sun’iy intellekt yordamida tahlil qilish uchun asosiy ma’lumot manbai sifatida ishlatiladi.

Cowrie honeypotni Linux muhitida o‘rnatish va sozlash SSH xizmatiga qaratilgan hujumlarni amaliy kuzatish imkonini beradi. Dastlab alohida Linux virtual mashinasi tayyorlanadi, tizim paketlari yangilanadi va kerakli kutubxonalar o‘rnatiladi. Keyin Cowrie uchun alohida foydalanuvchi yaratiladi, Python virtual muhiti sozlanadi va Cowrie pip orqali o‘rnatiladi.

Cowrie o‘rnatilgandan so‘ng cowrie.cfg konfiguratsiya fayli orqali honeypot nomi, SSH porti va Telnet sozlamalari belgilanadi. Cowrie ishga tushirilgach, tashqi SSH ulanishlari honeypotga yo‘naltiriladi. Natijada hujumchilar tomonidan amalga oshirilgan login-parol urinishlari, IP-manzillar, sessiya ma’lumotlari va terminal buyruqlari cowrie.log hamda cowrie.json fayllariga yozib boriladi.

Ushbu loglar keyinchalik statistik tahlil, grafik ko‘rinishda ifodalash va sun’iy intellekt yordamida chuqur tahlil qilish uchun asosiy ma’lumot manbai bo‘lib xizmat qiladi. Shu sababli Cowrie honeypotni Linux muhitida o‘rnatish jarayoni diplom loyiha ishining muhim amaliy bosqichi 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

ISSN: 2224-6878 | Pakistan Volume 6, No. 8.

IF: 15.9 | 2026 http://waerasia.org/index.php/ijtar

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.