**HONEYPOT TEXNOLOGIYASINING ASOSIY ISH   
PRINSIPLARI VA HUJUMNI YO‘NALTIRISH VA KUZATISH UCHUN TUZOQ YARATISH USULLARI**

**Annotatsiya:** Mazkur maqolada kiber xujumlarni oldini olish uchun honeypot texnologiyasining afzalliklar, tarmoq xavfsizligini ta‟minlovchi vositalar, honeypotlarni jismoniy yoki virtual ekanligiga qarab farqlash mumkinligi haqida ma‟lumotlar berilgan.

**KIRISH**

Axborot, Internet va kompyuter xavfsizligida aksariyat foydalanuvchilar tahdid, zaiflik va hujum tushunchalaridan tez-tez foydalanadilar. Biroq, aksariyat foydalanuvchilar tomonidan ularni almashtirish holatlari kuzatiladi.

Honeypot ozi nima? Birinchidan, honeypot kompyuter tizimidir. Honeypot - spam, fishing, DDoS yoki boshqa zararli usullardan foydalangan holda kompyuter tarmoqlariga hujum qilishga urinayotgan zararli hujumchilarni yolg‘on zaifliklar orqali jalb qilish uchun yaratilgan tuzoq sifatidagi kompyuter tizimi yoki ilovasi. Xaker ushbu tuzoqqa tushib qolsa, honeypot tizimi administratorlarga tajovuzkorning turi, u amalga oshirayotgan harakatlar va ko‘p hollarda hujumchini aniqlash haqidagi qimmatli ma’lumotlarni olish imkonini beradi. Unda xuddi haqiqiy kompyuter kabi fayllar, kataloglar mavjud. Biroq, kompyuterning maqsadi xakerlarni ularning xatti-harakatlarini kuzatish va kuzatish uchun unga tushishga jalb qilishdir. Shunday qilib, biz uni haqiqiy tizimga o'xshash soxta tizim sifatida belgilashimiz mumkin. Ular boshqa xavfsizlik tizimlaridan farq qiladi, chunki ular nafaqat ma'lum bir muammoga bitta yechim topadilar, balki turli xil xavfsizlik muammolarini qo'llashlari va ularga bir nechta yondashuvlarni topishlari mumkin. Masalan, ular buzilgan tizimdagi zararli harakatlarni qayd qilish uchun ishlatilishi mumkin, shuningdek, foydalanuvchilar uchun yangi tahdidlarni o'rganish va bu muammolardan qanday qutulish bo'yicha g'oyalarni yaratish uchun ishlatilishi mumkin.

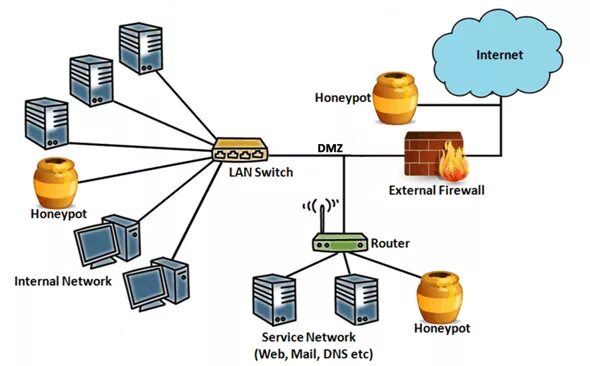
**ADABIYOTLAR TAHLILI VA METODOLOGIYA.**

Kiberxavfsizlik dunyosida honeypot tushunchasi odatda tizimning haqiqiy hatti-harakatlariga ega bo‘lgan, qasddan xavfsizlik bo‘shlig‘ini qoldiradigan va ularga kirishni istagan kiber jinoyatchilar haqida ma’lumot to‘plashni maqsad qilgan tuzoq tizimlari deb ataladi. Bu zaifliklar orqali kiberhujumlarni jalb qilishni maqsad qilib qo‘ygan kompyuter tizimi. U kiberhujumchilar kabi nishonga taqlid qilish va hujumga urinishlar, ishlash usullari haqida bilish yoki ularni boshqa nishonlardan chalg‘itish uchun ishlatiladi.

Barcha honeypotlarning asosiy maqsadi har xil turdagi dasturiy ta’minotga qarshi paydo bo‘ladigan hujumlarni aniqlash va razvedka ma’lumotlarini tahlil qilish va yaratish uchun hisobotlarni to‘plashdan iborat. Yig‘ilgan hisobotlardan keyinchalik tarmoq tahdidlariga qarshi profilaktika usullarini yaratishda foydalaniladi. Yuqorida aytib o‘tilganidek, honeypot tuzoq tizimidir. Ushbu tuzoq tizimlari ko‘pincha tarmoqqa ulangan virtual mashina yoki bulut serverida o‘rnatiladi. Shu bilan birga tizim va tarmoq ishtirokchilari tomonidan izolyatsiya qilingan bo‘lib, qat’iy nazorat qilinadi. Hujumchilarning e’tiboriga tushish uchun, honeypot maqsadli himoyasiz bo‘lishi zarur. Shu holatda uning zaif tomonlarini tajovuzkor aniqlaydi va ulardan foydalanishga harakat qiladi. Ushbu zaifliklar ilova ichidagi xavfsizlik tizimining bir qismi bo‘lishi mumkin. Keraksiz ochiq portlar, eskirgan dasturiy ta’minot versiyalari, zaif parol yoki eskirgan yadro kabilar ham tizim zaifliklaridan biri bo‘lishi mumkin.

**HONEYPOT TAVSIFI**

Honeypotlar ma’lum replikatsiya vektorlari va zararli dastur hujumlari signaturalaridan foydalanish orqali zararli dasturlarni aniqlash uchun ishlatiladi. USB xotira yoki flesh disklar kabi replikatsiya vektorlaridagi o‘zgarish belgilarini qo‘lda yoki drayverlardan nusxa oluvchi maxsus honeypotlar yordamida osongina tekshirish mumkin. Hujumchi o‘zining zaif nishonini topgandan so‘ng, u tizim yoki ilova ustidan ma’lum nazoratni qo‘lga kiritmaguncha hujumni boshlashga va imtiyozlarni oshirishga harakat qiladi. Xakerlarning ko‘pchiligi bilmaydigan narsa shundaki, honeypot ma’muri ularning har bir qadamini diqqat bilan kuzatib, hujumchidan joriy xavfsizlik siyosatini kuchaytirishga yordam beradigan ma’lumotlarni to‘playdi. Shuningdek, administrator, hodisa haqida darhol yuridik organlarga xabar berishi mumkin bo‘lib, bu ko‘pincha yuqori darajadagi korporativ tarmoqlarda sodir bo‘ladi. Aksariyat honeypotlar hujumchilarni haqiqiy tarmoqlarda joylashgan muhim ma’lumotlardan chalg‘itadigan tuzoq sifatida ishlaydi. Yana bir umumiy jihat shundaki, honeypotga ulanishning deyarli barcha urinishlari dushman deb hisoblanishi mumkin, chunki, odatda qonuniy foydalanuvchini ushbu turdagi tizimlar bilan bog‘lanishga undaydigan sabablar kam bo‘ladi.



**1-rasm. Honeypot arxitekturasi**

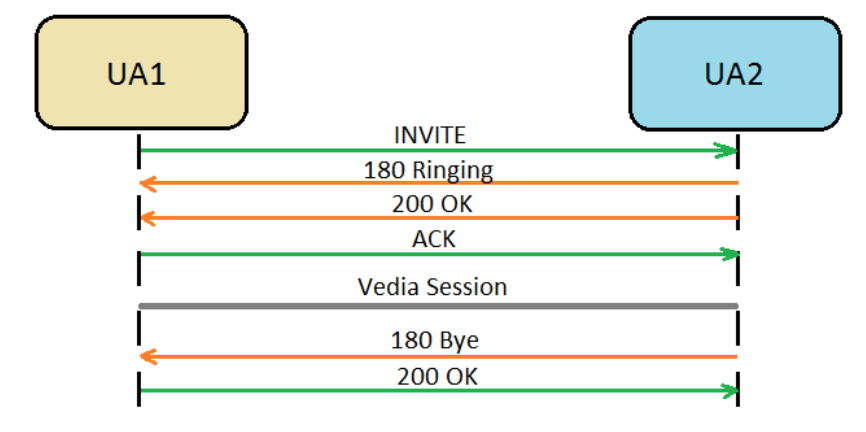
Honeypotni yaratilishida e’tibor qaratish lozim bo‘lgan muhim jihatlardan biri - ma’mur qanday qilib hujumchiga xakerlik qilish qiyin bo‘lishini bilishi kerak. Agar honeypotni buzish juda oson bo‘lsa ya’ni himoya qismiga e’tibor berilmasa, buzg‘unchi yoki Xakerlar qiziqishlarini yo‘qotishlari, hatto haqiqiy ishlab chiqarish tizimi bilan shug‘ullanmayotganliklarini tushunishlari ham mumkin. Bunday holda honeypot o‘z vazifasini bajara olmaydi. Boshqa tomondan, agar tizim juda kuchli himoyalangan bo‘lsa, har qanday hujumlarni to‘xtatish va hech qanday ma’lumot to‘play olmaslik holati yuzaga keladi. Shunday qilib, qiyinchilik nuqtai nazaridan, hujumchilarni osonlik va qiyinchilik o‘rtasidagi muvozanatni saqlagan holda jalb qilish haqiqiy vaziyatni simulyatsiya qilish uchun eng yaxshi kafolat bo‘ladi.

**SIP PROTOKOLIDAN FOYDALANGAN HOLDA TARMOQ XIZMATLARI UCHUN HONEYPOT-TUZOQLARNI ISHLAB CHIQISH**

SIP (Session Initiation Protocol) - foydalanuvchilarga ovozli va video qo'ng'iroqlarni amalga oshirish imkonini beruvchi protocol.

SIP dunyo bo'ylab odamlar Internet orqali shaxsiy kompyuterlar va mobil qurilmalar orqali muloqot qilish imkonini beradi. Internet-telefoniya muhim qismidir va VoIP (IP orqali ovoz) afzalliklarini ishlatish va boy muloqot tajribasiga ega bo'lish imkonini beradi. Ammo biz SIP dan olingan eng qiziqarli foyda aloqa xarajatlarini qisqartirishdir. SIP foydalanuvchilari orasida qo'ng'iroqlar (ovoz yoki video) butun dunyo bo'ylab bepul. Hech qanday chegara va cheklov qonunlari yoki ayblovlar yo‘q.

SIP protokoli orqali ikki mijoz o'rtasida aloqa o'rnatish misoli 2-rasmda ko'rsatilgan:



**2-rasm. SIP-dan foydalangan holda sessiyani o‘rnatish va tugatish bilan ikki mijoz o‘rtasidagi o‘zaro aloqa o‘rnatish**

UA1 (User Agent 1) UA2 bilan sessiya yaratmoqchi. Buning uchun u UA2 ga INVITE-xabarini, ya’ni sessiyaga qo‘shilish taklifini yuboradi.

Keyin UA2 telefoni jiringlay boshlaydi, bu haqda ma‘lumot UA1-ga 180 Ringing paketida yuboriladi. Agar UA2 qo‘ng'iroqqa javob bersa, muvaffaqiyatli ulanish haqidagi ma'lumotlarni o'z ichiga olgan paket UA1 ga yuboriladi. UA1 ACK paket yuboradi, bu UA2 ga UA1 oldingi xabarni muvaffaqiyatli qabul qilgani haqida ma’lumot beradi. Shuningdek, ushbu paketda mavjud ulanishning oxirgi parametrlari yuboriladi.

Qachonki qaysidir foydalanuvchi telefonni qo‘ysa, ikkinchisiga *180 Bye* paketi yuboriladi. Bunga javoban 200 OK xabari jo‘natiladi. Seans tugadi.

**HONEYPOTNI O'RNATISH VA SOZLASH**

Tadqiqot uchun Honeypot - Conpot tanlandi. Ushbu mahsulotni o‘rnatish va sozlash juda oson; u global tarmoqlarda qo'llaniladigan ko'pgina xizmatlarni taklif qiladi.

Ushbu Honeypotni o'rnatish uchun bulutli server tanlandi.

Server xususiyatlari:

Operatsion tizim: Ubuntu 20.04

Protsessor: 1x2,8 gigagerts

RAM: 1 GB

Ma'lumotlarni saqlash uchun 15 GB SSD ishlatiladi.

Bu xususiyatlar Conpotning barqaror ishlashi uchun yetarli.

Tuzoqni o'rnatish bosqichlari:

1. Kerakli paketlarni yangilashingiz va o'rnatishingiz kerak:

$ sudo apt update

$ sudo apt-get install git libsmi2ldbl smistrip libxslt1-dev python3.8-dev

libevent-dev default-libmysqlclient-dev

$ sudo apt-get install python3-pip

$ sudo pip3 install virtualenv

$ sudo pip install --upgrade pip

$ sudo pip install --upgrade setuptools

$ sudo pip install cffi==1.14.0

2. Keyinchalik, siz githubdan repozitoriyni klonlashingiz kerak va conpot papkasiga o‘tishingiz kerak:

$ git clone https://github.com/mushorg/conpot

3. Yakuniy bosqich - buyruq orqali paketni o'rnatish:

$ sudo python3 setup.py install

Endi siz "tuzoq" ni buyruq bilan ishga tushirishingiz mumkin:

$ sudo conpot -f -t default

Shablon sifatida PLC Siemens S7-200ning standart “default” shabloni tanlandi. Default holatida, xizmatlar nostandart portlarda ishlaydi.

Masalan, HTTP serveri 80 o'rniga 8800 portida, FTP serveri 21 o'rniga 2121 portida ishlaydi.

Conpotning standart portlarda ishlashini ta'minlash uchun ***authbind*** utilitasidan foydalanish zarur.

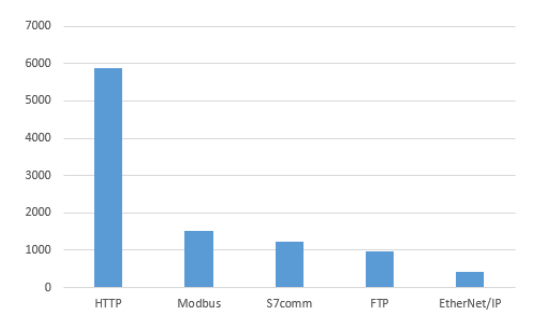
Muvaffaqiyatli ishga tushirilgandan so'ng, honeypot turli xil protokollar yordamida unga ulanishlarni yozib olishni boshlaydi va ***cmd***da ushbu ulanishlar haqidagi ma'lumotlarni ko'rsatadi.



**3-rasm. Ulanishlar haqida ma’lumotlar chiqishi**

**NATIJALAR**

Tadqiqot o'tkazish uchun Conpot bulutli serverda ishga tushirildi. Ma'lumotlarni yig'ish 7 kun davom etdi.



**4-rasm. Turli protokollar yordamida ulanganlar soni**

Yig'ilgan ma'lumotlarga asoslanib, biz qaysi protokolga tez-tez hujum qilinayotgani, shuningdek, tajovuzkor tizimimizga hujum qilganda qanday usullardan foydalanishi haqida xulosa chiqarishimiz mumkin.

**XULOSA**

Xulosa sifatida aytish mumkinki dinamik kiberxavfsizlik vositalari sifatida Honeypotlar ko‘p hollarda namoyon bo‘ladi, ularning turlari har biri o‘ziga xos tarzda ajralib turadi va o‘ziga xos maqsadlarga xizmat qiladi. Ushbu farqlar ko‘pincha turli mezonlardan kelib chiqadi, bu ularning maqsadi, ularni amalga oshirish metodologiyasi yoki ular qarshi turish uchun mo‘ljallangan o‘ziga xos tahdid landshafti bilan bog‘liq. Binobarin, eng mos honeypot turini tanlash muhim qaror bo‘lib, bir nechta muhim omillarni diqqat bilan ko‘rib chiqqandan keyin qabul qilinishi kerak. Taroziga soladigan birinchi omil tarmoqning hozirgi holatidir. Chunki tarmoq topologiyasini, masshtabini va u joylashgan muhim aktivlarini baholash muhim ahamiyatga ega.