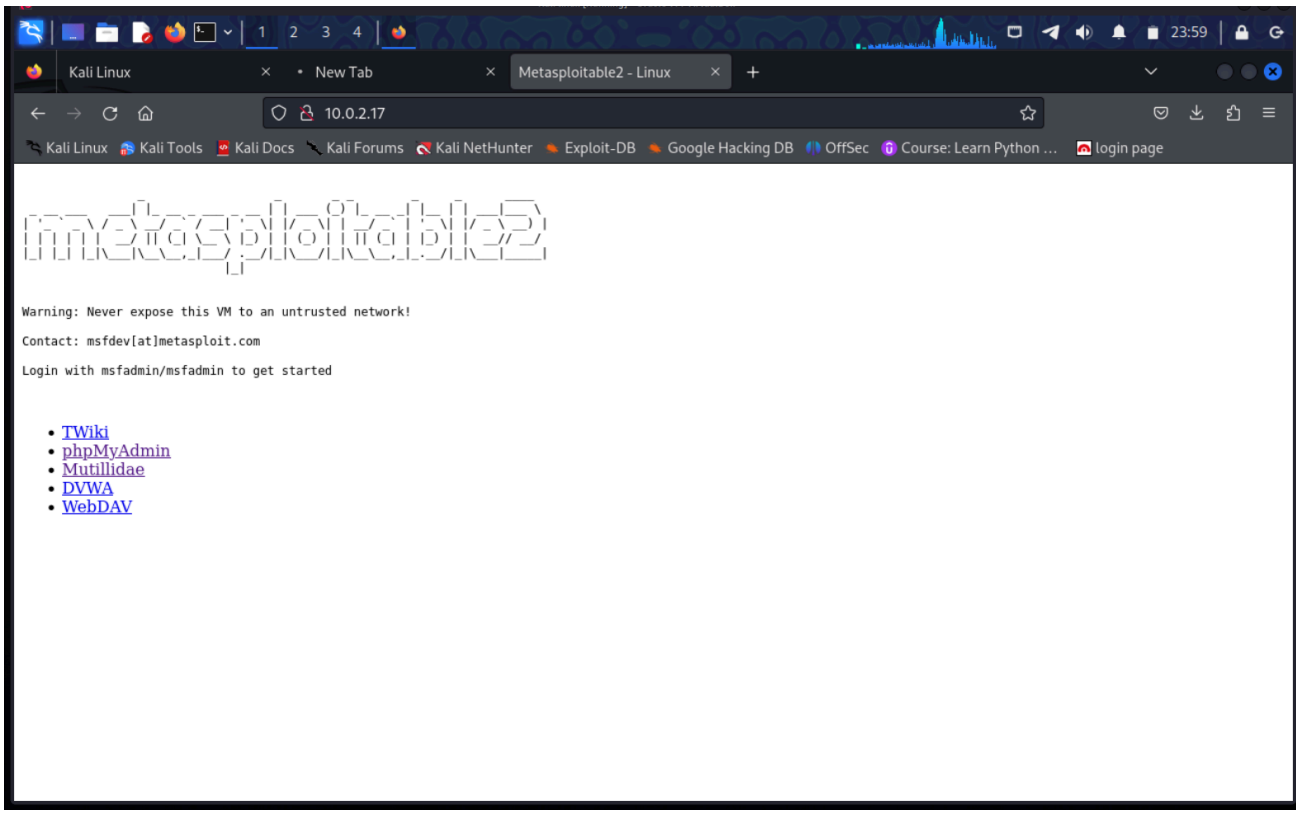
Gibrid Kiberxavfsizlik kursi

BUZIB KIRISH SINOVI HISOBOTI

Oybek Boltaboyev



Muqaddima

Ushbu hisobot muallifning berilgan vzifani qanchalik bajarganini tasdiqlovchi hujjat hisoblanib, bundagi amallar professionallar tomonidan bajarilgan bo'lib, real hayotda o'zboshimchalik bilan takrorlanmasin.

Oybek Boltaboyev

Maqsad: Ushbu buzib kirish sinovining maqsadi metasploitable 2 tizimidagi zaifliklarni, ularning exploit darajasini va bular bu=ilan keladigan xatar darajalarni aniqlash va xabar qilishdan iborat.

Ko’lami: Ushbu sinovning ko’lami Metasploitable 2 muhitini to’liq qamrab oladi. Testlar tarmoqni skanerlash, zaifliklarni baholash va aniqlangan zaifliklarni ekspluatatsiya qilishni o’z ichiga oladi.

Uslubiyat

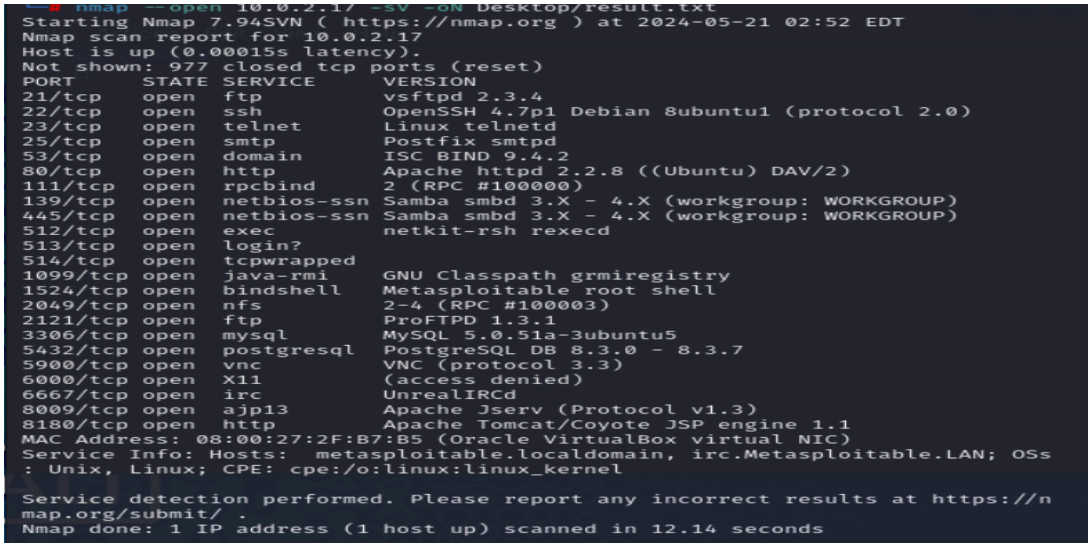
Ma’lumot yig’ish

Foydalanilgan vositalar:metasploit, msfconsole, exploit-db.com, Nmap

Dastlabki bosqichda nishon tizimi haqida ma’lumot yig’iladi. Nmap vositasida ochiq portlar va xizmatlarni aniqlash uchun tarmoq skanerlanadi.

Buyruq:

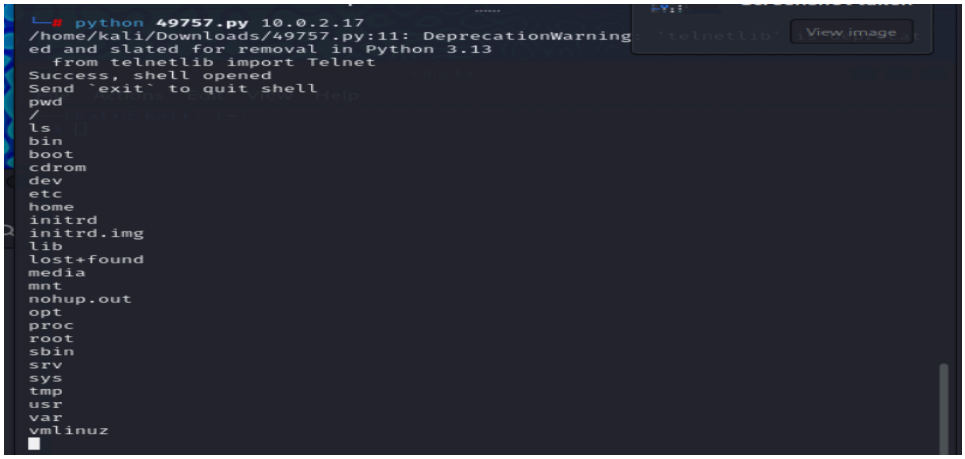
Natija:



Buyruq to’g’ri bajarilishi uchun terminalda to’liq imtiyoz olish talab qilinadi. Natija bizga Nmap aniqlay olgan ociq portlarni namoyish etadi. Quyida har bir port uchun mos zaiflik aniqlanadi va tizim egallanadi. Agar biz zaiflikar saqlanadigan ma’lumotlar bazasidan topilgan portlar bo’yicha ma’lumot izlasak bizga kerakli bo’lgan zaiflikni yuklab olib, qo’llashimiz mumkin

1-zaiflik. Vsftpd backdoor buyruq bajarilishi

https://www.exploit-db.com/download/49757 havola orqali ushbu port uchun backdoorning python faylini terminalda ishga tushuramiz:



Xatar: yuqori

Tavsiya: vsftpd ning 2.3.4 versiyasi backdoor zaifligini saqlagani tufayli, xatarni yumshatishning mumkin bo'lgan eng yaxshi yo'li so'nggi versiyagacha yangilashdir.

2-zaiflik. Noreal ircd backdoor buyruq bajarilishi

Irc xizmati 666 portda ishlayapti. Uning ba'zi versiyalarida backdoor o'rnatilganini va hujumchilar shu backdoorga bog'lana olinishini aniqladik.

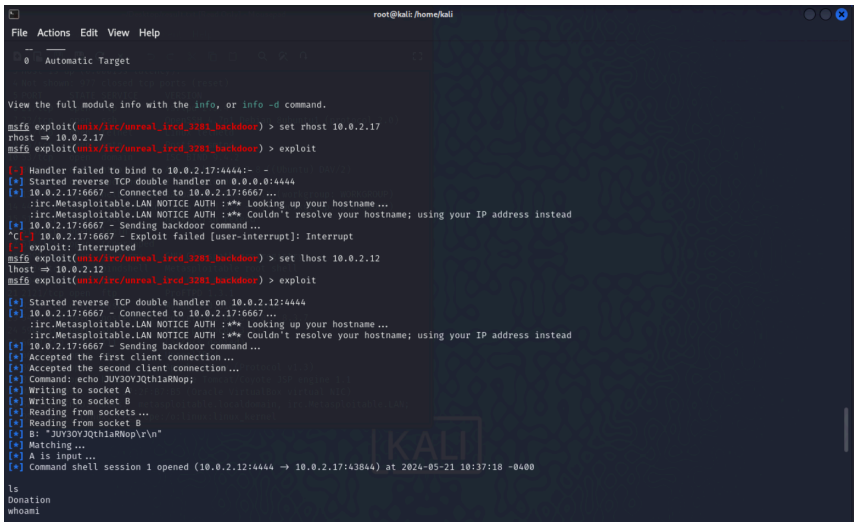
Exploit.

1.Bu xizmatni exploit qilish uchun to'g'ridan to'g'ri metasploit modulidan foydalanamiz.

2.Modulning irc backdoor idan foydalanish va masofaviy mezbon ip ni o'rnatish.

3. Masofadan ishlatiladigan yuklamani sozlash.

4. Bu yerda biz qobiq hosil qiladigan va bizning hujum ip imiz bilan bog'laydigan cmd/unix/reverse yuklamasidan foydalanamiz



Xatar. Yuqori

Tavsiya. Qo’lga olingan backdoor root darajasida. Shuning uchun servis vesiyasi yangilanishi kerak yoki port yopilishi kerak.

3-zaiflik. Distcc kod bajarilishi.

Tavsif.

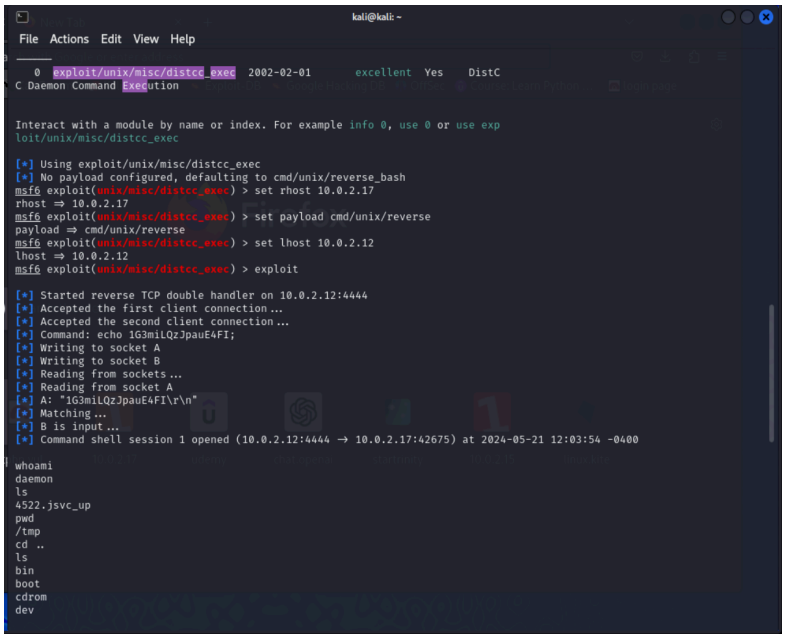
Distcc bu tarmoqdagi bir nechta mashinalar bo’ylab c, c++ va c/c++ ob’ektlarining tuzilishini tarqatish dasturi. Bu xizmat 3632 portda ishlaydi. Bu dasturning ba’zi versiyalarida zaiflik mavjud.

Exploit

1. msfconsole dan foydalanamiz.

2. Mashinalar ip sini sozlab chiqamiz.

3. Exploit buyruqlarini muvaffaqiyatli kiritganimizdan keyin, biz daemon imtiyozli qobiqqa ega bo’lamiz



Xatar. Yuqori

Tavsiya. Usbu xavfsizlik zaifligini yumshatishni yo'li yo xizmat uchun yamash bajarilguncha portni yopish. Agar yuqoriroq va yamalgan distcc versiyasi mavjud bo'lmasaki tezda o'rnatilishi shart bo'lgan.

Xulosalar

Tizimdagi xatarlar aniqanishi uchun mashina hujumchi nuqtayi nazari tomonidan hujumga uchrashi zarur. Ma'lumotlar aniqlangach, biz osongina exploitlarni exploitlar bazasidan qidirib topishimiz va u exploitlarni tizimda sinab ko'rishimiz mumkin. Nihoyat biz biz zaifliklarni o'tkazib yubormaganimizga amin bo'lishimiz uchun biz avtomatlashtirilgan xavfsizlik scannerlardan foydalanamiz, ammo ularning natijalari zaifliklarni tanlashning yagona mezoni bo'lmasligi kerak. Sababi ular ba'zan tizimni zararlab qo'yishi va noto'g'ri natijalar bilan ta'minlashi mumkin.

So'ngso'z o'rnida bu xatarlarni yumshatish uchun eng yaxshi tavsiya bu tizimni yangilangan holatda saqlash va sozlamalarni to'g'ri amalga oshirishdir.