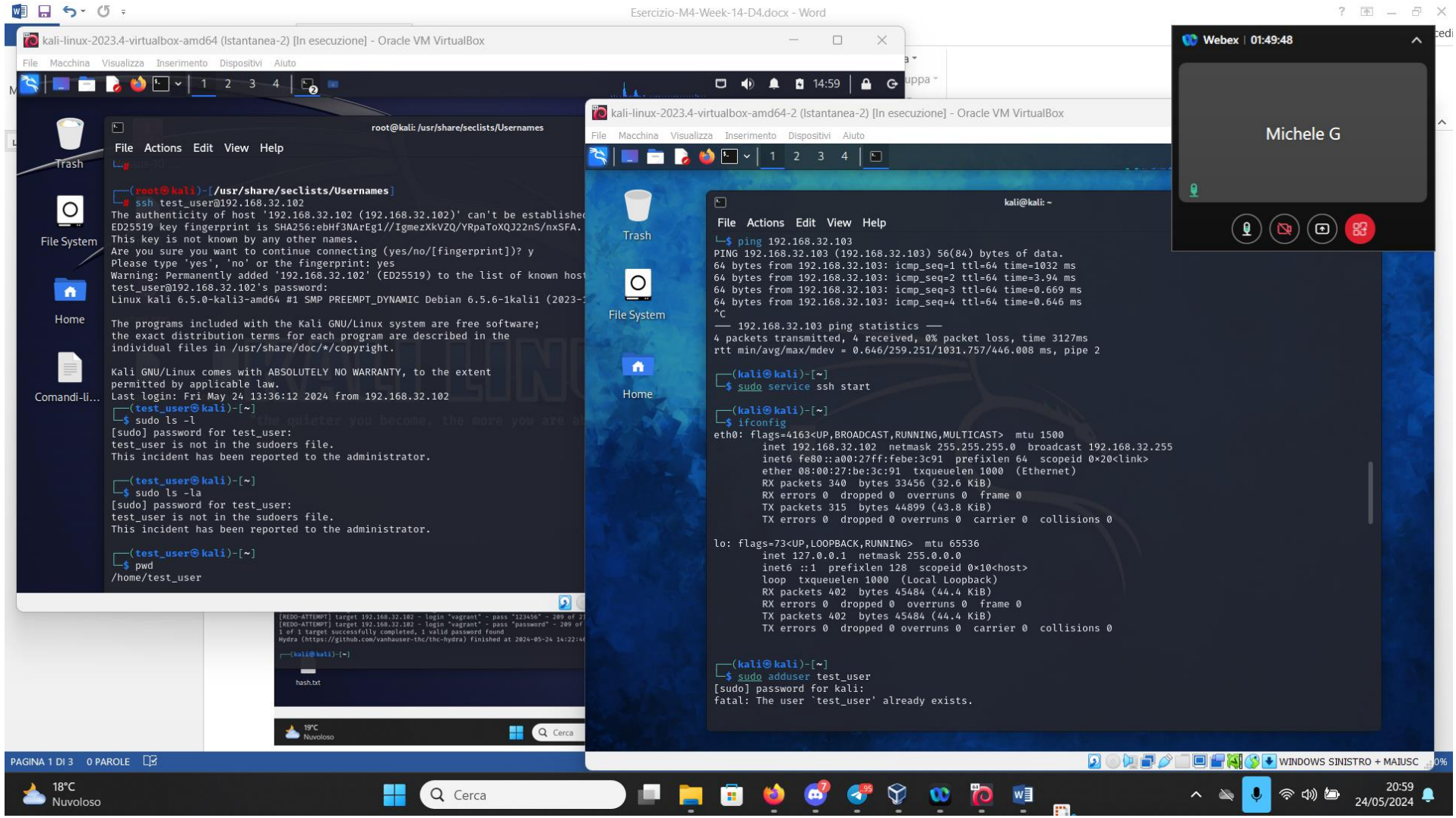
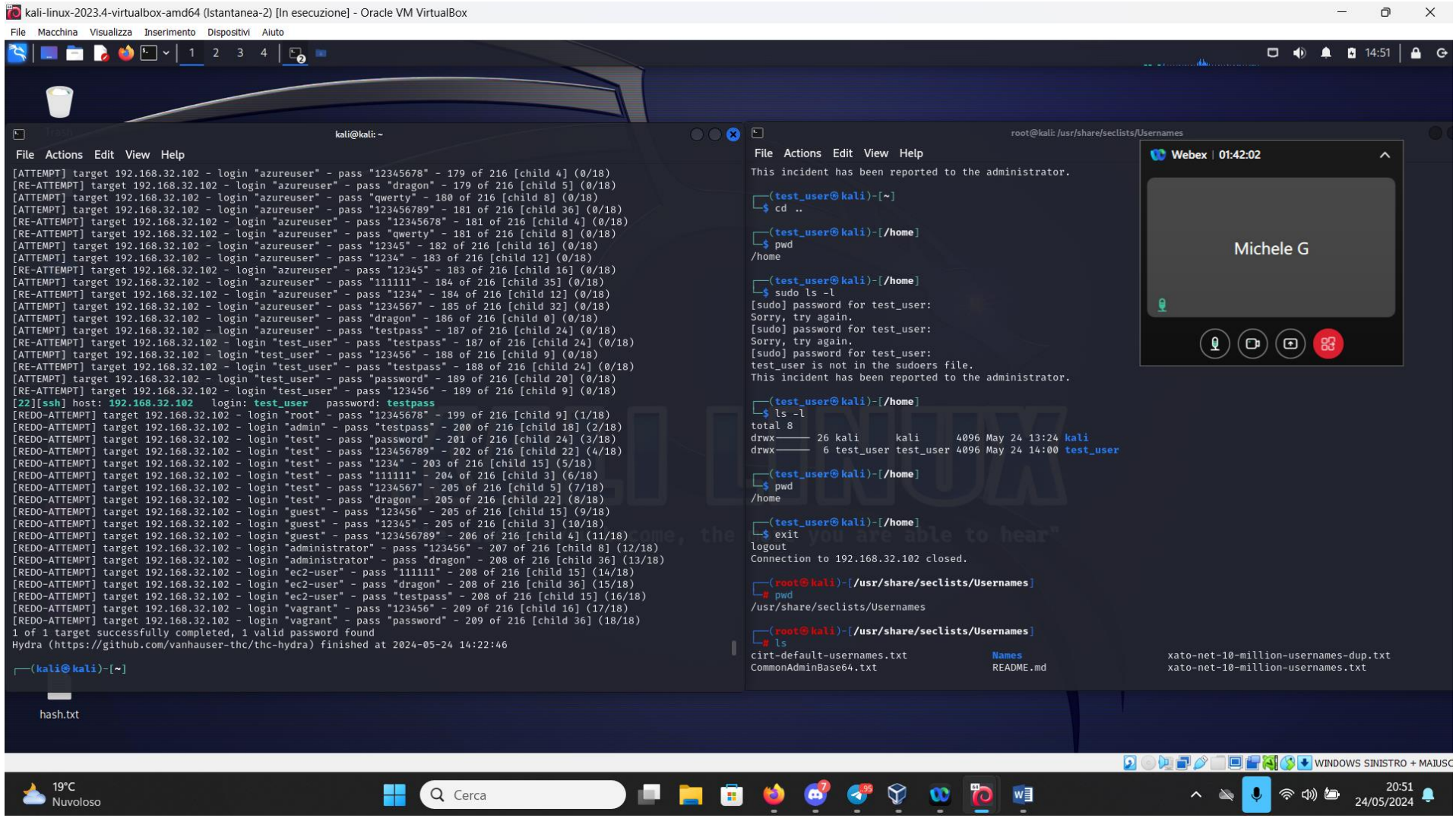
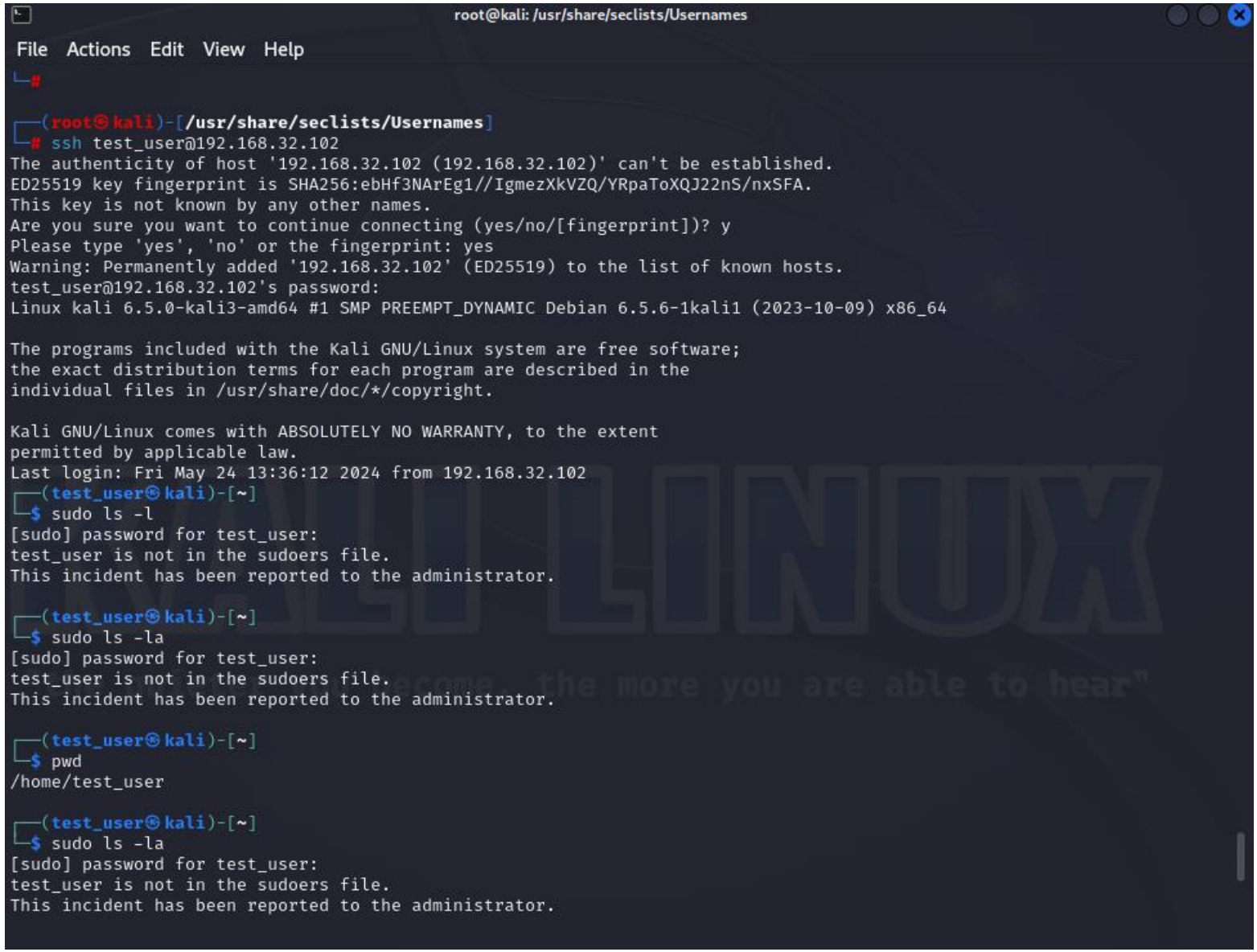
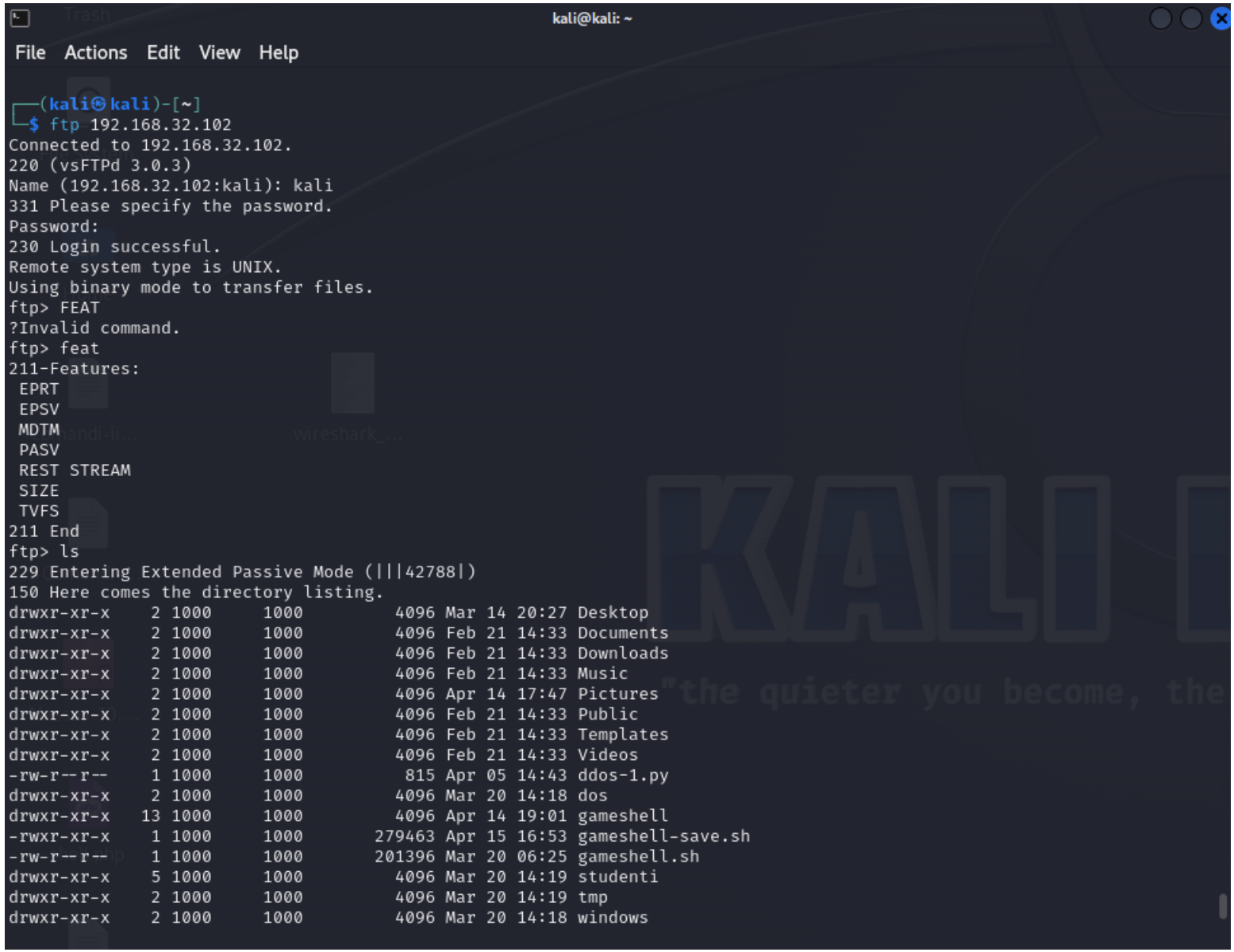

Esercizio-M4-Week-14-D4.docx - Word
kali-linux-2023.4-virtualbox-amd64 (Istantanea-2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
14:59
Trash
File System
Home
Comandi-li...
root@kali: /usr/share/seclists/Usernames
File Actions Edit View Help
(root㉿kali)-[/usr/share/seclists/Usernames]
ssh test_user@192.168.32.102
The authenticity of host '192.168.32.102 (192.168.32.102)' can't be establishe
ED25519 key fingerprint is SHA256:ebHf3NArEg1//IgmezXkVZQ/YRpaToXQJ22nS/nxSFA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.32.102' (ED25519) to the list of known host
test_user@192.168.32.102's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May 24 13:36:12 2024 from 192.168.32.102
(test_user㉿kali)-[~]
$ sudo ls -l
[sudo] password for test_user:
test_user is not in the sudoers file.
This incident has been reported to the administrator.
(test_user㉿kali)-[~]
$ sudo ls -la
[sudo] password for test_user:
test_user is not in the sudoers file.
This incident has been reported to the administrator.
(test_user㉿kali)-[~]
$ pwd
/home/test_user
kali-linux-2023.4-virtualbox-amd64-2 (Istantanea-2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
$ ping 192.168.32.103
PING 192.168.32.103 (192.168.32.103) 56(84) bytes of data.
64 bytes from 192.168.32.103: icmp_seq=1 ttl=64 time=1032 ms
64 bytes from 192.168.32.103: icmp_seq=2 ttl=64 time=3.94 ms
64 bytes from 192.168.32.103: icmp_seq=3 ttl=64 time=0.669 ms
64 bytes from 192.168.32.103: icmp_seq=4 ttl=64 time=0.646 ms
^C
— 192.168.32.103 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3127ms
rtt min/avg/max/mdev = 0.646/259.251/1031.757/446.008 ms, pipe 2
(kali㉿kali)-[~]
$ sudo service ssh start
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.32.102 netmask 255.255.255.0 broadcast 192.168.32.255
inet6 fe80::a00:27ff:febe:3c91 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:be:3c:91 txqueuelen 1000 (Ethernet)
RX packets 340 bytes 33456 (32.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 315 bytes 44899 (43.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 402 bytes 45484 (44.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 402 bytes 45484 (44.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali㉿kali)-[~]
$ sudo adduser test_user
[sudo] password for kali:
fatal: The user `test_user' already exists.
Webex | 01:49:48
Michele G
PAGINA 1 DI 3 0 PAROLE
WINDOWS SINISTRO + MAIUSC
18°C Nuvoloso
Cerca
20:59
24/05/2024


kali-linux-2023.4-virtualbox-amd64 (Istantanea-2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
[ATTEMPT] target 192.168.32.102 - login "azureuser" - pass "12345678" - 179 of 216 [child 4] (0/18)
[RE-ATTEMPT] target 192.168.32.102 - login "azureuser" - pass "dragon" - 179 of 216 [child 5] (0/18)
[ATTEMPT] target 192.168.32.102 - login "azureuser" - pass "qwerty" - 180 of 216 [child 8] (0/18)
[ATTEMPT] target 192.168.32.102 - login "azureuser" - pass "123456789" - 181 of 216 [child 36] (0/18)
[RE-ATTEMPT] target 192.168.32.102 - login "azureuser" - pass "12345678" - 181 of 216 [child 4] (0/18)
[RE-ATTEMPT] target 192.168.32.102 - login "azureuser" - pass "qwerty" - 181 of 216 [child 8] (0/18)
[ATTEMPT] target 192.168.32.102 - login "azureuser" - pass "12345" - 182 of 216 [child 16] (0/18)
[ATTEMPT] target 192.168.32.102 - login "azureuser" - pass "1234" - 183 of 216 [child 12] (0/18)
[RE-ATTEMPT] target 192.168.32.102 - login "azureuser" - pass "12345" - 183 of 216 [child 16] (0/18)
[ATTEMPT] target 192.168.32.102 - login "azureuser" - pass "111111" - 184 of 216 [child 35] (0/18)
[RE-ATTEMPT] target 192.168.32.102 - login "azureuser" - pass "1234" - 184 of 216 [child 12] (0/18)
[ATTEMPT] target 192.168.32.102 - login "azureuser" - pass "1234567" - 185 of 216 [child 32] (0/18)
[ATTEMPT] target 192.168.32.102 - login "azureuser" - pass "dragon" - 186 of 216 [child 0] (0/18)
[ATTEMPT] target 192.168.32.102 - login "azureuser" - pass "testpass" - 187 of 216 [child 24] (0/18)
[RE-ATTEMPT] target 192.168.32.102 - login "test_user" - pass "testpass" - 187 of 216 [child 24] (0/18)
[ATTEMPT] target 192.168.32.102 - login "test_user" - pass "123456" - 188 of 216 [child 9] (0/18)
[RE-ATTEMPT] target 192.168.32.102 - login "test_user" - pass "testpass" - 188 of 216 [child 24] (0/18)
[ATTEMPT] target 192.168.32.102 - login "test_user" - pass "password" - 189 of 216 [child 20] (0/18)
[RE-ATTEMPT] target 192.168.32.102 - login "test_user" - pass "123456" - 189 of 216 [child 9] (0/18)
[22][ssh] host: 192.168.32.102 login: test_user password: testpass
[REDO-ATTEMPT] target 192.168.32.102 - login "root" - pass "12345678" - 199 of 216 [child 9] (1/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "admin" - pass "testpass" - 200 of 216 [child 18] (2/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "test" - pass "password" - 201 of 216 [child 24] (3/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "test" - pass "123456789" - 202 of 216 [child 22] (4/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "test" - pass "1234" - 203 of 216 [child 15] (5/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "test" - pass "111111" - 204 of 216 [child 3] (6/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "test" - pass "1234567" - 205 of 216 [child 5] (7/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "test" - pass "dragon" - 205 of 216 [child 22] (8/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "guest" - pass "123456" - 205 of 216 [child 15] (9/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "guest" - pass "12345" - 205 of 216 [child 3] (10/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "guest" - pass "123456789" - 206 of 216 [child 4] (11/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "administrator" - pass "123456" - 207 of 216 [child 8] (12/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "administrator" - pass "dragon" - 208 of 216 [child 36] (13/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "ec2-user" - pass "111111" - 208 of 216 [child 15] (14/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "ec2-user" - pass "dragon" - 208 of 216 [child 36] (15/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "ec2-user" - pass "testpass" - 208 of 216 [child 15] (16/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "vagrant" - pass "123456" - 209 of 216 [child 16] (17/18)
[REDO-ATTEMPT] target 192.168.32.102 - login "vagrant" - pass "password" - 209 of 216 [child 36] (18/18)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-24 14:22:46
(kali㉿kali)-[~]
hash.txt
root@kali: /usr/share/seclists/Usernames
File Actions Edit View Help
This incident has been reported to the administrator.
(test_user㉿kali)-[~]
$ cd ..
(test_user㉿kali)-[/home]
$ pwd
/home
(test_user㉿kali)-[/home]
$ sudo ls -l
[sudo] password for test_user:
Sorry, try again.
[sudo] password for test_user:
Sorry, try again.
[sudo] password for test_user:
test_user is not in the sudoers file.
This incident has been reported to the administrator.
(test_user㉿kali)-[/home]
$ ls -l
total 8
drwx------ 26 kali kali 4096 May 24 13:24 kali
drwx------ 6 test_user test_user 4096 May 24 14:00 test_user
(test_user㉿kali)-[/home]
$ pwd
/home
(test_user㉿kali)-[/home]
$ exit
logout
Connection to 192.168.32.102 closed.
(root㉿kali)-[/usr/share/seclists/Usernames]
pwd
/usr/share/seclists/Usernames
(root㉿kali)-[/usr/share/seclists/Usernames]
ls
cirt-default-usernames.txt Names xato-net-10-million-usernames-dup.txt
CommonAdminBase64.txt README.md xato-net-10-million-usernames.txt
Webex | 01:42:02
Michele G
WINDOWS SINISTRO + MAIUSC
19°C Nuvoloso
Cerca
20:51 24/05/2024


root@kali: /usr/share/seclists/Usernames
File Actions Edit View Help
└─#
┌──(root㉿kali)-[/usr/share/seclists/Usernames]
└─# ssh test_user@192.168.32.102
The authenticity of host '192.168.32.102 (192.168.32.102)' can't be established.
ED25519 key fingerprint is SHA256:ebHf3NArEg1//IgmezXkVZQ/YRpaToXQJ22nS/nxSFA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.32.102' (ED25519) to the list of known hosts.
test_user@192.168.32.102's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) x86_64
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May 24 13:36:12 2024 from 192.168.32.102
┌──(test_user㉿kali)-[~]
└─$ sudo ls -l
[sudo] password for test_user:
test_user is not in the sudoers file.
This incident has been reported to the administrator.
┌──(test_user㉿kali)-[~]
└─$ sudo ls -la
[sudo] password for test_user:
test_user is not in the sudoers file.
This incident has been reported to the administrator.
┌──(test_user㉿kali)-[~]
└─$ pwd
/home/test_user
┌──(test_user㉿kali)-[~]
└─$ sudo ls -la
[sudo] password for test_user:
test_user is not in the sudoers file.
This incident has been reported to the administrator.


kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.32.102
Connected to 192.168.32.102.
220 (vsFTPd 3.0.3)
Name (192.168.32.102:kali): kali
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> FEAT
?Invalid command.
ftp> feat
211-Features:
 EPRT
 EPSV
 MDTM
 PASV
 REST STREAM
 SIZE
 TVFS
211 End
ftp> ls
229 Entering Extended Passive Mode (|||42788|)
150 Here comes the directory listing.
drwxr-xr-x 2 1000 1000 4096 Mar 14 20:27 Desktop
drwxr-xr-x 2 1000 1000 4096 Feb 21 14:33 Documents
drwxr-xr-x 2 1000 1000 4096 Feb 21 14:33 Downloads
drwxr-xr-x 2 1000 1000 4096 Feb 21 14:33 Music
drwxr-xr-x 2 1000 1000 4096 Apr 14 17:47 Pictures
drwxr-xr-x 2 1000 1000 4096 Feb 21 14:33 Public
drwxr-xr-x 2 1000 1000 4096 Feb 21 14:33 Templates
drwxr-xr-x 2 1000 1000 4096 Feb 21 14:33 Videos
-rw-r--r-- 1 1000 1000 815 Apr 05 14:43 ddos-1.py
drwxr-xr-x 2 1000 1000 4096 Mar 20 14:18 dos
drwxr-xr-x 13 1000 1000 4096 Apr 14 19:01 gameshell
-rwxr-xr-x 1 1000 1000 279463 Apr 15 16:53 gameshell-save.sh
-rw-r--r-- 1 1000 1000 201396 Mar 20 06:25 gameshell.sh
drwxr-xr-x 5 1000 1000 4096 Mar 20 14:19 studenti
drwxr-xr-x 2 1000 1000 4096 Mar 20 14:19 tmp
drwxr-xr-x 2 1000 1000 4096 Mar 20 14:18 windows