CS 536 Lab Answers 4

Prashant Ravi — ravi18@purdue.edu

October 30, 2016

Problem 1

1 Ping App

Ping results without tunnel :

```
Round trip time was :   0 ms
Client received datagram from xinu11.cs.purdue.edu (128.10.3.61)
```

On the pingd server we see these results.
Ping results with tunnel : Same.
Analysis: These results were the same as for "with" tunnel case. So, I didn't include them. I think the proximity of the servers(XINU systems) prevents us from noticing any big change in these numbers, since the packet size is small. The tunnel app may give more info.

2 Tunnel App

Without tunnel

```
xinu14 70 $ ./traffic_rcv.o 4554
Completion time: 1.090000 seconds
Application bitrate: 918.348624 pps
Application bitrate: 7677064.220183 bps
```

```
xinu13 82 $ ./traffic_snd.o xinu14.cs.purdue.e
Completion time: 1.090000 seconds
Application bitrate: 917.431193 pps
Application bitrate: 7677064.220183 bps
```

With tunnel

```
xinu14 69 $ ./traffic_rcv.o 4554
Completion time: 1.089000 seconds
Application bitrate: 919.191919 pps
Application bitrate: 7684113.865932 bps
```

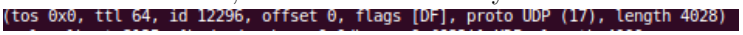
```
xinu13 81 $ ./traffic_snd.o xinu11.cs.purdue.edu 58489 1000 1000 1000
Completion time: 1.089000 seconds
Application bitrate: 918.273646 pps
Application bitrate: 7684113.865932 bps
```

Claim: As we can see there is no difference, with or without a tunnel.
Analysis: The assumption we hold is that the vpn server is in close proximity to the real server we intend to interact with. If this assumption does not hold then neither does the claim.

Problem 3

The TTL is 64 for udp on this system. The TTL to cisco.com is 239 and 60 to google.com. They are different from what we expected during sniffing. Yes, they can vary across operating systems. Since we were using linux to linux udp during traffic-rcv we got 64. However, 239 was received when pinging cisco.com

which means they are probably using Red Hat OS. Very much like a hacker, I was just now able to tell what OS cisco systems is using by just checking the TTL values.Thus,you can tell the OS from TTL values, that's information that can be useful to hacker, since TTL values vary across OSes.



TOS is set to 0x0(off). And DF are the fragment bits, which stands for don't fragment.

Problem 4 = Bonus Problem

Please check gui-wechat.c. It is a gtk2+ application. Instructions are in the file. Please make sure to type hostname port to initiate chat. 'C', 'N' must be typed on receiver wechat to accept/decline. Basically, all instructions of the terminal wechat are supported in the gui.