Jimmy Tran

Panther ID: 002-11-0395

Bourgeois

7 April 2017

Assignment 4

Notes: I actually had to install Scapy 3.0.0 and a fair amount of other junk for it to work on Windows at all. If my values tend to be odd or otherwise unusual, I blame that and may note as such below.

1a) Default ttl is 64. It can be modified. A small value will cause a host to resend backups too quickly. A large one will make a host take too long to resend.

1b) No flags are shown. Any normal character (letter or number) or combinations of those seem to be possible in the flag field.

1c) It is a valid address. It is the IP normally used by a host who has not been identified by another host yet that is sending/receiving; a default IP in other words.

1d) The packet will go to 127.0.0.1. It is actually the localhost or loopback IP address. Sending a packet here will just send it to the source itself.

1e) IP is displayed in the proto field as it is the protocol field, and the variable we are seeing is a packet that falls under that protocol.

2a) The proto field now says UDP.

2b) The default values of the UDP layer are sport=domain, dport=domain, len=none, and chksum=none.

3a) No. Nothing else changed (although I know it should since 8.8.8.8 is a Google Public DNS).

3b) For a packet to reach 8.8.8.8, it probably needs to be rerouted across some number of other routers before reaching the final destination.

4a) DNS is on the application layer rather than the network layer.

4b) UDP is used by DNS to transfer packets. In our case specifically, we are only sending one small packet so TCP is not needed.

4c) Yes. We can still use TCP as it can still access DNS without issues. In fact, TCP is used when many packets are needed to be sent rather than the few that UDP can handle at most.