

[exec] Raven: how does traceroute actually work?

[exec] is there something in the TCP header or so

[Raven] exec, i'll explain

[snider] traceroute isnt ovetr TCP

[angst] something about a TTL field I know that

[Raven] ooh, i can feel a spontaneous lecture coming!

(Samcon) snider: strange its probably with the ripper

[Raven] is anyone logging this?

[angst] I know what it is in my head, just cant type what I want to say :)

(Samcon) im

[Raven] who else is logging?

(Samcon) just a sec

[snider] samcon, well it is something with the identification and auth of it

(Samcon) im always logging btw

[tcs] are u holding a tutorial session ?

[Raven] ok, so the topic of this spontaneous lecture is...

[Raven] how does traceroute works

[Cypher] lecture?

[Raven] Cypher, spontaneous

[FrEEkY] raven untill phoneabuse.com is working I just refer people to BSRF

[snider] yea, although we have explained the matter a million times in here

[Raven] ok try to be quiet please

[Raven] so anyway, first of all, what is traceroute?

[Raven] traceroute traces the route that a packet goes through to get to a certain ip / hostname

[Raven] it's especially good to detect network problems

[Raven] if you're having trouble connecting to a certain host, you could run traceroute and see where the problem is

[Raven] where the chain stops

[Raven] any questions so far?

[Olaf] there is a great command in widows tracert

[Olaf] is it related?

[Raven] Olaf, in windows you can type tracert from dos

[Raven] in unix/linux, you can type traceroute

[Raven] or tracert if you make an alias

[Raven] :-)

[Olaf] my poor linux

[Raven] anyway for windows, there's also www.sampspade.org

[Raven] ok, we're continuing

[Raven] so anyway, this is what traceroute does

[Raven] now, how does it work?

(Samcon) traceroute is the thing with the packet that gets +1 node every time no ?

[Raven] ok, first of all, i have to explain a little about TCP/IP

?~ joins [|The_Crow| (*!Itsaia@PTlink-23723.teleweb.pt)]

[Raven] TCP/IP packets can be divided into two types

[Raven] a) ip packets

[Raven] b) icmp packets

[Raven] each packet has a header part and a data part

?~ nick change [Cypher ~ Cypher[awayY]]

[Raven] the header contains info about the sender, the target and any other information that is necessary so the packet would get to it's destination

[Raven] now, icmp packets have a header, and a data

[Raven] there are 13 (i think) types of icmp packets

[Raven] one of them, for example, is ICMP_ECHO_REQUEST

[Raven] which is used for ping

[Raven] however icmp is mainly used for errors

[Raven] now, there are ip packets

[Raven] ip packets have a header and a data part

[Raven] the header contains the source and destination ip

[Raven] and a few other values

[Raven] like the TTL, for example

[Raven] (i'll explain later)

[Raven] the data part is either a TCP or a UDP packet

[Raven] these two terms are explained in bsr's tcpip tutorial

[Raven] any questions so far?

[Raven] no? good.

[Raven] ok, so this TTL value serves a great role in killing misrouted packets

[Raven] supposed something happens and packets start looping or wandering around the net endlessly

[Raven] that'd be a serious waste of bandwidth, right?

[Olaf] yes

[FrEEkY] mmhmm

[Raven] so this is why the ip header contains a TTL value

[Raven] and so does the icmp header, i think

[Olaf] it decreases

[Raven] i don't remember

[Raven] anyway this TTL value is decreased whenever a packet goes through a router

[Raven] TTL = Time To Live

(Samcon) thats what i meant

[Raven] whenever a packet goes through a router, the TTL value is decreased by one

[angst] ICMP (Internet Control Message Protocol) BTW.... :)

[Raven] that way, if a packet goes through too many hops on the way, it gets killed

[Raven] and an icmp error is sent back to the sender

[Raven] windows 95 sends packets with a TTL value of 32

[Raven] i don't know about win 98

[Raven] anyway sometimes you'll have to go through more than 32 hops, so you'll get an error and windows will send the packet again with TTL = 64

[Raven] now, here's how traceroute works:

[Raven] first of all it sends out a packet with TTL = 1

[Raven] the packets goes through the first hop, and dies

[Raven] that router sends back an icmp error, and that way we can determine his ip / hostname

[Raven] because we can tell who is sending the packet by looking at the icmp header

[Raven] then, traceroute sends a packet with TTL = 2

[Raven] it travels through the first hop (which we already know) and dies in the second

[Raven] we get an error from the second router, thus revealing it's ip

[Raven] this goes on until the packet reaches it's destination

?^ quits [Olaf (*!-----@194.65.83.PTlink-11626)] (Ping timeout)

?^ quits [tcs (*!tcs@204.42.41.PTlink-12468)] (Quit: I'll check the logs...)

[Raven] that way, we can tell where our packets go through by getting an error message from each hop

[Raven] that's all. that's how traceroute works

[Raven] :-)

[Raven] end of spontaneous lecture

[exec] cool