

Forum:[Hack Forums](#)

Thread: [Need help with TCP hijack](#)

ryanleh - June 29, 2016, 10:13 am

Hi, I'm helping develop a program that will hijack the TCP connection between two hosts on a ICS and continue conversations with both of them separately (this is for demonstration purposes to convince higher-ups of a need for more security on these devices). I'm using ettercap to ARP MITM the targets and scapy to do all of the sniffing and processing. All the coding for grabbing the seq number and continuing the connection is fine but for the life in me I can't figure out a way to stop ettercap from forwarding packets between the hosts. The idea is that once I have the info I need (seq number from TCP and the protocol) I cut off the hosts from talking to eachother but nothing seems to work.... I've tried iptables and ettercap filters. Any ideas on how to accomplish this?

Phizo - July 1, 2016, 4:08 am

This attack basically works by you masquerading as the router. I am unsure whether there is some functionality within Ettercap to toggle packet forwarding, but what you can do is inhibit your kernel from routing. What OS are you using? If Linux, what is the value of `/proc/sys/net/ipv4/ip_forward`? Intuitively, 0 is off and 1 is on. If it is 1, then do `echo 0 > /proc/sys/net/ipv4/ip_forward` as root and see how that goes. Another solution is to instead use arpspoof, which does not handle packet forwarding.

xComplexUnity - July 1, 2016, 4:11 am

Toggle packet forwarding :)