

Forum:[Hack Forums](#)

Thread: [Router Access/Socks Proxy Using Dark Comet](#)

granger - July 22, 2012, 10:51 pm

So here is my dilemma. I have a theoretical work around for it, but it seems more complicated than I think it is.

Scenario.

I have two separate networks on two different internet connections isolated from each other.

Both are using standard linksys routers with default gateway subnets of 192.168.1.xxx. The admin page for both routers is located at 192.168.1.1 on each network.

We'll call network 1 the attacking network and network 2 the victim network. Let's also assume that the victim network has no open ports on the router.

I have a test laptop setup on the victim network which is infected with DC reporting back to the attacking network. Because the victim network is behind a router though, starting up a socks proxy would theoretically be moot since the victim router does not have the correct port open.

In order to gain access to the router from the compromised host, I envision the use of netcat/winrelay/fpipe in order to create another reverse shell back to the attacking network in order to redirect a web browser on the attacking network to the router admin page of the victim network.

I'm not sure if my theory is totally off base or if there is an easier way to do it without raising an alarm (i.e. using RD to log into the router page), but it's food for thought. Or you could call me an idiot and tell me there is already a prebuilt way to do this in dark comet. Either would be fine with me ?