

Re: Scan for "outsider" Pcs on network

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2006-09/msg00033.html>

- *From:* "Eric W Hacker" <[focus@xxxxxxxxxxxxx](mailto:xxxxxxx)>
 - *Date:* Sun, 17 Sep 2006 20:30:29 -0400
-

On 9/12/06, Craig Chamberlain <craig.chamberlain@xxxxxxx> wrote:

Or spoofing a MAC address, which I find works OK even when the host being spoofed is connected to the same port at the same time, and works OK when the MAC is tied to a DHCP reservation (the switch has no way of knowing there area actually two NICS attached).

Echoing and extending what Mr. Chamberlain said: ETHERNET IS NOT, BY ITSELF, SECURABLE.

I apologize for feeling the need to shout, but there are many, many people who do not seem to get this. The only authentication a switch can use is the MAC address. MAC addresses are just as insecure as credit card numbers (I'll leave that rant for another time).

802.1x does not secure one's Ethernet network. Statically configuring switch ports by MAC address does not secure one's Ethernet network. MAC addresses can be manipulated in many ways, but software bridging is the most fun.

I've been hoarding some of this for well over a year in hopes that I'd write a nice polished white paper, but that doesn't seem to be happening. Some might have said these things elsewhere. I don't claim to be the first, but it appears that this line of questioning was making an assumption that Ethernet could be secured. Enjoy:

Trick #1, The Hijack the Printer

Printers don't typically support 802.1x. so they'll probably be on a switch port set up to only accept their mac address. Enter Mr. Ethical Hacker (no relation [1]) with his multi port, unobtrusive Soerkis OpenBSD Box (SOB) set up as a bridge. He drops it inline with the printer and departs. The SOB is set up to watch the traffic on the wire, and take on the IP address and MAC of the printer behind it when it needs to talk. It uses filtering to pull out its own traffic before bridging packets to the printer, so the printer never knows SOB is there. The switch never knows either, because at layers two and three,

Re: Scan for "outsider" Pcs on network

SOB appears just to be a bit more talkative than usual printer.

SOB can be set up to try several different tunneling methods to get back out and call home to Mr. Ethical Hacker. Of course, if the network is really secure, printers don't get to talk to much of anything. Yeah right, it's a safe bet not too many of you are that secure, but just in case....

Trick #2 Hijack a Desktop's LAN port.

Same deal as number one, except now SOB has got someone who will surely have access to network applications. If the network has 802.1x and it is set up to reauthenticate every minute or so, as it should, then SOB will have to wait until the supplicant on the desktop is authenticated, but it can be patient. SOB can also sniff out all the unencrypted traffic to the desktop and might get user privileges to use for data mining. The user will likely have access to the Internet, at least through a proxy, so SOB will almost surely be able to get out. Again, it may have to wait until the user has authenticated with the proxy, but how many proxies are set up to authenticate each transaction?

Once SOB has control of the IP address of a system and can ride on the rights that IP address is granted through the system user's authorization, then it is very unlikely that one can keep SOB from getting data out of the network. I'll leave the proof of that for some other time.

Trick #3, Hijack LAN ports for VoIP phones.

Currently almost all VoIP deployments are not using enough encryption, even if the particular system installation could support it, because the overhead is too high. VoIP without encryption is a free-for-all. Drop in SOB between a VoIP phone and the switch, and one likely can listen in on all calls, make calls directly to other phones, intercept calls, transfer calls elsewhere, etc.

Some VoIP phones do VLAN tagging and have the desktop plug into the phone which then tags the traffic to be on separate VLANs on the same switch port. This doesn't slow down SOB one bit. BSD can do VLAN tagging. As a matter of fact, if the switch ports are not locked down by VLAN, then SOB might be able to access even more of the network. Got one of those quarantine networks that's allowed out for when contractors plug in? SOB will just ride both the inside and the outside VLANs at the same time. That's probably not a likely scenario, but it sure would be fun.

Summary.

I hope I've demonstrated that Ethernet in itself is not securable. If not, I have even more tricks up my sleeve for a later day. MAC address

Re: Scan for "outsider" Pcs on network

authentication is all that is provided with each packet. If one needs layer two security, one had better use a different protocol or layer something else on top of Ethernet..

Peace,
Eric Hacker, CISSP

Some might say that I was born with an apronym for a surname, but I think that I've still much work ahead of meto earn that title.

[1] I'd love for this to be me, but frankly I haven't had the time and opportunity to put all this together and probably never will. I've done some exploratory work and the theory is, I beleive, sound.

Test Your IDS

Is your IDS deployed correctly?

Find out quickly and easily by testing it with real-world attacks from CORE IMPACT.

Go to http://www.coresecurity.com/index.php5?module=Form&action=impact&campaign=intro_sfw to learn more.
