

RE: Dhcp security

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2005-01/0160.html>

skander.ben.mansour_at_accenture.com

Date: 01/28/05

Date: Fri, 28 Jan 2005 10:04:19 +0100

To: <focus-ms@securityfocus.com>

Hello Paul,

This might be overkill in your environment but:

Another idea is to leverage your AD infrastructure to authenticate users using the 802.1x protocol.

The 802.1x protocol only allows authenticated users to connect to a switch port, or can grant limited connectivity to unauthenticated users.

The following Microsoft link shows how to set this up for a wireless network.

<http://www.microsoft.com/technet/archive/community/columns/security/5min/5min-303.msp>

Setting up a 802.1x wired network requires:

- a 802.1x client on the users workstations/laptops
- a 802.1x compatible switch (supported by most Cisco switches)
- a RADIUS server (I believe W2K Server includes a RADIUS service, which then proxies the authentication to the AD domain server)

It provides the advantage of scaling to large deployments, compared to manual MAC address/switch port configuration.

Regarding controlling virus spreading from uncontrolled devices, some vendors, including Cisco, provide solutions to ensure that only properly configured/patched/AV updated devices can connect to the network:

http://www.cisco.com/warp/public/cc/so/neso/sqso/csdni_wp.htm

"Cisco Trust Agent–Software that resides on an endpoint system. The trust agent collects security state information from multiple security software clients, such as anti–virus clients, and then communicates this information to Cisco network access devices, which enforce admission control. Cisco has licensed trust agent technology to its anti–virus co–sponsors so that it can be integrated with their security software client products. The trust agent will also be integrated with the Cisco Security Agent to enforce access privileges based on an endpoint's operating system patch level. Cisco Security Agent, a day–zero host

SecurityFocus Microsoft: RE: Dhcp security

protection software solution, will assess the operating system version, patch, and hot fix information and will communicate this information to the Cisco Trust Agent. Hosts that are not running the proper patches may be given limited access or denied network access."

I hope this helps.

Best Regards,

Skander Ben Mansour, CISA CISSP

<http://www.benmansour.net>

-----Original Message-----

From: JJ Cummings [mailto:JJ.Cummings@greatcleaners.com]

Sent: vendredi 21 janvier 2005 04:51

To: Paul Aviles; focus-ms@securityfocus.com

Subject: RE: Dhcp security

Paul,

One way "depending on how many clients you are servicing" would be to create MAC (layer 2) based reservations, and only allow that exact number of addresses in the available scope (again, each with a specific MAC reservation). This does not, however, prevent static IP addressing of unauthorized clients. For this you would need some hardware ACL stuff, either on a switch capable of MAC filtering or route the traffic through a security device (layer 2 again) before allowing network access. All of this would have to be layer 2 at this point.

AND / OR...

Another option that could also be used in conjunction with the aforementioned would be VLAN membership rubbish. By this I mean configure a specific VLAN to have DHCP services on it; you then setup the NIC on the client to be a member of this specific VLAN (most new decent NICs allow for this) and configure the switchport/switch to allow only traffic from this specific VLAN. I say use this in conjunction with the first, because someone could figure out the VLAN ID and simply set it, much like a static...so use both for a multi-layer approach (always a good idea "defense and depth").

I will think about this some more and give more specific info if you like, I am fairly fried from sleep deprivation right now so my brain functions may not be functioning as they should :-P

Regards,

JJC

``The lyf so short, the craft so long to lerne.'' - Chaucer

-----Original Message-----

From: Paul Aviles [mailto:paviles@adjoined.com]

Sent: Wednesday, January 19, 2005 3:30 PM

To: focus-ms@securityfocus.com

Subject: Dhcp security

I have a weird question maybe. Is there a way to prevent our DHCP from giving leases to computers not in our domain? I don't want anyone that walks in to just connect and have the possibility of a network viruses getting loose. Is this possible?

My setup is a typical AD 2K environment, simple domain no empty root.

Thanks

Paul

SecurityFocus Microsoft: RE: Dhcp security

This message is for the designated recipient only and may contain privileged, proprietary, or other confidential information.
