

RE: How to find a changing IP on ethernet network

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-03/0003.html>

From: David Gillett (gillettdavid_at_fhda.edu)

Date: 02/28/04

To: "'Bhavani Suresh'" <bhavani.suresh@adnoc-dist.co.ae>, "'Gideon T. Rasmussen, CISSP, CISM, CFSO, SCSA'" <grasmussen@infostruct.net>
Date: Fri, 27 Feb 2004 17:17:51 -0800

If you're using Cisco Catalyst switches, this feature is called "port security". Enable it, tell it how many MAC addresses to allow per port, and whether, when this number is exceeded, to issue an SMTP trap to your Network Management package, or shut down the switch port.

Of course, if you're using some other equipment, you need to find out what features, if any, that equipment offers.

David Gillett

> -----Original Message-----

> From: Bhavani Suresh [<mailto:bhavani.suresh@adnoc-dist.co.ae>]

> Sent: Wednesday, February 25, 2004 2:36 AM

> To: Gideon T. Rasmussen, CISSP, CISM, CFSO, SCSA;

> security-basics@securityfocus.com

> Subject: RE: How to find a changing IP on ethernet network

>

>

>

> Following up this..i want to know at the network level any

> software can

> bind the MAC Addresses to the ports (and to take current MAC Addresses

> in the network automatically)so that no new ip address can be

> allocated

> without the consent of the network admin. This will also

> ensure security

> so that non one just plugs in a pc or laptop..

>

> Any idea..

>

> -----Original Message-----

> From: Gideon T. Rasmussen, CISSP, CISM, CFSO, SCSA

> [<mailto:lists@infostruct.net>] Sent: Saturday, February 21, 2004 20:12

> To: security-basics@securityfocus.com

> Subject: Re: How to find a changing IP on ethernet network

>

RE: How to find a changing IP on ethernet network

SecurityFocus BASICS: RE: How to find a changing IP on ethernet network

>
>
> Ivan,
>
> *This is an interesting situation. Here are a few possible
> ways to address it:*
>
> 1. *Send an e-mail to the user community explaining the
> problem and asking them to leave their IP address
> configurations alone.*
>
> 2. *In case you don't know, as the new system boots it
> announces its IP address to the network. If another system
> already has that IP address, it will reply and the new system
> will shut down the interface running the duplicate IP.*
>
> a. *From the new system, run the arp command (arp -a).*
>
> C:\> arp -a
>
> *Interface: 192.168.2.100 --- 0x20002
> Internet Address Physical Address Type
> 192.168.2.1 00-06-25-c0-93-65 dynamic*
>
> *This will list the IP address and associated MAC (hardware)
> address (e.g. 00-06-25-c0-93-65).*
>
> b. *Now all you need to do is find out which system has that
> MAC address:*
>
> C:\> ipconfig /all (output abbreviated)
>
> *Physical Address. : 00-06-25-c0-93-65*
>
> 3. *You could also use tcpdump or windump
> (<http://windump.polito.it>) to sniff the network traffic for
> that specific IP and view the resulting dump file with
> Ethereal (<http://www.ethereal.com>). This is a bit advanced
> for the average user.*
>
> *If you have any additional questions, please do not hesitate
> to contact
> me.*
>
> *Kind regards,*
>
> *Gideon*
>
> *Gideon T. Rasmussen*
> *CISSP, CISM, CFSO, SCSCA*
> *Boca Raton, FL*

RE: How to find a changing IP on ethernet network

SecurityFocus BASICS: RE: How to find a changing IP on ethernet network

> *gideon@infostruct.net*
>
> *National Security Awareness Day – September 10, 2004 – Are you aware?*
>
> *Subject: How to find a changing IP on ethernet network*
> *From: Ivan Andres Hernandez Puga <ivan.hernandez@globalsis.com.ar>*
> *Date: Fri, 20 Feb 2004 11:54:29 -0300*
> *To: security-basics@securityfocus.com*

>
> *Hello. I have a client with a simple Ethernet network with*
> *HUB's connecting and there is one person that is changing*
> *it's IP and creating*
>
> *conflicts. What would you do to track down that person? i*
> *mean, to find who does that?*

>
> *Thanks!*
>
> *Ivan Hernandez*

> -----
> -----

> ---
> *Free trial: Astaro Security Linux -- firewall with Spam/Virus*
> *Protection*
>
> *Protect your network with the comprehensive security solution that*
> *integrates six applications for ease of use and lower TCO.*
>
> *Firewall – Virus protection – Spam protection – URL blocking – VPN*
> *– Wireless security.*
>
> *Download 30-day evaluation at:*
> *http://www.securityfocus.com/sponsor/Astaro_security-basics_040219*

> -----
> -----

>
> *****
> *Please note that our domain name has been changed to: adnoc-dist.ae;*
> *Hence please change the email ID to reflect the new domain name. This*
> *communication may contain confidential information. If you are not the*
> *intended recipient, then please inform us immediately. Adnoc*
> *Distribution–Tel:02-6771300 Fax:02-6722322*
> *Email:webmaster@adnoc-dist.ae*
> *Website: www.adnoc-dist.ae*
> *This message was scanned @ Adnoc distribution*

SecurityFocus BASICS: RE: How to find a changing IP on ethernet network

>
> *****

>
> *****

> *Please note that our domain name has been changed to:*
> *adnoc-dist.ae; Hence please change the email ID to reflect*
> *the new domain name.*
> *This communication may contain confidential information.*
> *If you are not the intended recipient, then please inform us*
> *immediately.*
> *Adnoc Distribution-Tel:02-6771300 Fax:02-6722322*
> *Email:webmaster@adnoc-dist.ae Website: www.adnoc-dist.ae*
> *This message was scanned @ Adnoc distribution*

>
> *****

>
> -----
> -----
> -----
> -----
>

