

Re: Threat – Operating System Detected

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-09/0039.html>

From: Steven L Umbach (*n9rou_at_nospam-comcast.net*)

Date: 09/07/05

Date: Wed, 7 Sep 2005 00:11:09 -0500

Number one use a properly configured firewall to protect your network from untrusted networks and harden your operating systems to disable unneeded services such as SNMP if you are not using it or at least disable it on computers where it is not needed. Enable other best security practices such as enforcing complex passwords for the domain, physically securing high value computers including domain controllers, enable auditing for at least domain controllers and sensitive servers/computers, strongly consider requiring smart cards for sensitive accounts such as domain administrators, and having a strategy to keep current with critical security updates. Sure you can also have an attacker on the inside of your network but reviewing of security logs should help you quickly identify such an attacker and best practices for security can extremely limit what such an attacker can do. Weak passwords, non physically secured computers, and untrained/inept users administrators are by far your biggest risk.

Ipssec can also be used in the domain to protect domain assets. Ipssec can require computer authentication before communications are allowed between two computers and then insure integrity and confidentiality of the data. Ipssec policies must be tested thoroughly before implementing in a live domain. The free downloadable Windows 2000 Security Hardening Guide and the Threats and Countermeasures Guide [geared toward 2003/XP but still good info] can help you to secure your domain. The links below may help. ---
Steve

<http://www.microsoft.com/downloads/details.aspx?FamilyID=15E83186-A2C8-4C8F-A9D0-A0201F639A56&Disp>

<http://www.microsoft.com/technet/security/topics/serversecurity/tcg/tcgch00.msp>

<http://www.microsoft.com/technet/security/default.msp> --- TechNet

Security main page

<http://www.microsoft.com/technet/security/topics/architectureanddesign/ipsec/default.msp>

--- domain isolation using ipsec

<http://www.bookpool.com/sm/0735620334> --- Assessing Network Security

"Neil" <Neil@discussions.microsoft.com> wrote in message
news:6AAB2EDD-0415-4771-947C-E1A70DCE86DE@microsoft.com...

> *What could be the solution to clear this violation shown below?*

>

> **THREAT:**

> *Several different techniques can be used to identify the operating system*

- > (OS) running on a host. A short description of these techniques is
- > provided
- > below. The specific technique used to identify the OS on this host is
- > included in the RESULTS section of your report.
- > 1) TCP/IP Fingerprint: The operating system of a host can be identified
- > from
- > a remote system using TCP/IP fingerprinting. All underlying operating
- > system TCP/IP stacks have subtle differences that can be seen in their
- > responses to specially–crafted TCP packets. According to the results of
- > this
- > "fingerprinting" technique, the OS version is among those listed below.
- > Note that if one or more of these subtle differences are modified by a
- > firewall or a packet filtering device between the scanner and the host,
- > the
- > fingerprinting technique may fail. Consequently, the version of the OS may
- > not be detected correctly. If the host is behind a proxy–type firewall,
- > the
- > version of the operating system detected may be that for the firewall
- > instead of for the host being scanned.
- > 2) NetBIOS: Short for Network Basic Input Output System, an application
- > programming interface (API) that augments the DOS BIOS by adding
- > special functions for local–area networks (LANs). Almost all LANs for PCs
- > are based on the NetBIOS. Some LAN manufacturers have even extended
- > it, adding additional network capabilities. NetBIOS relies on a message
- > format called Server Message Block (SMB).
- > 3) PHP Info: PHP is a hypertext pre–processor, an open–source,
- > server–side,
- > HTML–embedded scripting language used to create dynamic Web
- > pages. Under some configurations it is possible to call PHP functions like
- > phpinfo() and obtain operating system information.
- > 4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts,
- > routers, and the networks to which they attach. The SNMP service
- > maintains Management Information Base (MIB), a set of variables (database)
- > that can be fetched by Managers. These include
- > "MIB_II.system.sysDescr" for the operating system.