OpenVAS Scan Report

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details

Hosts which were alive and responding during test	1
Number of security holes	0
Number of security warnings	3
Number of security notes	24
Number of false positives	0

Host List

Host(s)	Possible Issue
163.26.17.1	Security warning(s)

[return to top]

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
163.26.17.1	domain (53/tcp)	Security note(s)
163.26.17.1	http (80/tcp)	Security note(s)
163.26.17.1	epmap (135/tcp)	Security warning(s)
163.26.17.1	netbios-ssn (139/tcp)	Security note(s)
163.26.17.1	microsoft-ds (445/tcp)	Security note(s)
163.26.17.1	ms-wbt-server (3389/tcp)	Security note(s)
163.26.17.1	general/tcp	Security warning(s)
163.26.17.1	ssh (22/tcp)	No Information
163.26.17.1	netbios-ns (137/udp)	Security warning(s)
163.26.17.1	domain (53/udp)	Security note(s)
163.26.17.1	unknown (49152/tcp)	Security note(s)
163.26.17.1	unknown (49153/tcp)	Security note(s)
163.26.17.1	unknown (49154/tcp)	Security note(s)
163.26.17.1	unknown (49155/tcp)	Security note(s)
163.26.17.1	unknown (49156/tcp)	Security note(s)
163.26.17.1	unknown (49162/tcp)	Security note(s)
163.26.17.1	general/SMBClient	Security note(s)
163.26.17.1	general/CPE-T	No Information

Security Issues and Fixes: 163.26.17.1

Type	Port	Issue and Fix
Informational	domain (53/tcp)	Overview: A DNS Server is running at this Host. A Name Server translates domain names into IP addresses. This makes it possible for a user to access a website by typing in the domain name instead of the website's actual IP address. Risk factor : None OID : 1.3.6.1.4.1.25623.1.0.100069
Informational	domain (53/tcp)	Microsoft DNS server seems to be running on this port.

		Internal hostname disclosed (0.in-addr.arpa/SOA/IN): win-rjugyqkbv68 OID : 1.3.6.1.4.1.25623.1.0.100950
Informational	domain (53/tcp)	Microsoft DNS server seems to be running on this port. Internal hostname disclosed (255.in-addr.arpa/SOA/IN): win-rjugyqkbv68 OID : 1.3.6.1.4.1.25623.1.0.100950
Informational	http (80/tcp)	A web server is running on this port OID : 1.3.6.1.4.1.25623.1.0.10330
Informational	http (80/tcp)	The remote web server type is : Microsoft-IIS/7.0 OID : 1.3.6.1.4.1.25623.1.0.10107
Informational	http (80/tcp)	\nServer: Microsoft-IIS/7.0\nOperating System Type: Windows Longhorn\nX-AspNet-Version: 2.0.50727\nX-Powered-By: ASP.NET OID : 1.3.6.1.4.1.25623.1.0.101018
Warning	epmap (135/tcp)	 Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Solution : filter incoming traffic to this port. Risk factor : Low OID : 1.3.6.1.4.1.25623.1.0.10736
Informational	netbios-ssn (139/tcp)	An SMB server is running on this port OID : 1.3.6.1.4.1.25623.1.0.11011
Informational	microsoft-ds (445/tcp)	A CIFS server is running on this port OID : 1.3.6.1.4.1.25623.1.0.11011
Informational	microsoft-ds (445/tcp)	It was possible to log into the remote host using user defined login/password combinations : OID : 1.3.6.1.4.1.25623.1.0.10394
Informational	microsoft-ds (445/tcp)	 Overview: It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication. Detected SMB workgroup: WORKGROUP Detected SMB server: Windows Server (R) 2008 Enterprise 6.0 Detected OS: Windows Server (R) 2008 Enterprise 6002 Service Pack 2 OID : 1.3.6.1.4.1.25623.1.0.102011
Informational	ms-wbt-server (3389/tcp)	 The Microsoft Remote Desktop Protocol (RDP) is running at this host. Remote Desktop Services, formerly known as Terminal Services, is one of the components of Microsoft Windows (both server and client versions) that allows a user to access applications and data on a remote computer over a network. Risk factor : None OID : 1.3.6.1.4.1.25623.1.0.100062
Warning	general/tcp	 The remote host accepts loose source routed IP packets. The feature was designed for testing purpose. An attacker may use it to circumvent poorly designed IP filtering and exploit another flaw. However, it is not dangerous by itself. Solution : drop source routed packets on this host or on other ingress routers or firewalls.

		Risk factor : Low OID : 1.3.6.1.4.1.25623.1.0.11834
Informational	general/tcp	Microsoft IIS Webserver Version 7.0 was detected on the host OID : 1.3.6.1.4.1.25623.1.0.900710
Informational	general/tcp	ICMP based OS fingerprint results: HP JetDirect ROM A.03.17 EEPROM A.04.09 (accuracy 80%) HP JetDirect ROM A.05.03 EEPROM A.05.05 (accuracy 80%) HP JetDirect ROM F.08.01 EEPROM F.08.05 (accuracy 80%) HP JetDirect ROM F.08.08 EEPROM F.08.05 (accuracy 80%) HP JetDirect ROM F.08.08 EEPROM F.08.20 (accuracy 80%) HP JetDirect ROM G.05.34 EEPROM G.05.35 (accuracy 80%) HP JetDirect ROM G.06.00 EEPROM G.06.00 (accuracy 80%) HP JetDirect ROM G.07.02 EEPROM G.07.17 (accuracy 80%) HP JetDirect ROM G.07.02 EEPROM G.07.20 (accuracy 80%) HP JetDirect ROM G.07.02 EEPROM G.08.04 (accuracy 80%) HP JetDirect ROM G.07.19 EEPROM G.07.20 (accuracy 80%) HP JetDirect ROM G.07.19 EEPROM G.08.03 (accuracy 80%) HP JetDirect ROM G.07.19 EEPROM G.08.04 (accuracy 80%) HP JetDirect ROM G.08.08 EEPROM G.08.04 (accuracy 80%) HP JetDirect ROM G.08.21 EEPROM G.08.21 (accuracy 80%) HP JetDirect ROM H.07.15 EEPROM H.08.20 (accuracy 80%) OID : 1.3.6.1.4.1.25623.1.0.102002
Warning	netbios-ns (137/udp)	The following 3 NetBIOS names have been gathered : WIN-RJUGYQKBV68 = This is the computer name registered for workstation services by a WINS client. WORKGROUP = Workgroup / Domain name WIN-RJUGYQKBV68 = Computer name The remote host has the following MAC address on its adapter : 00:1f:d0:12:c0:bb If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port. Risk factor : Medium CVE : CAN-1999-0621 OID : 1.3.6.1.4.1.25623.1.0.10150
Informational	domain (53/udp)	 Overview: A DNS Server is running at this Host. A Name Server translates domain names into IP addresses. This makes it possible for a user to access a website by typing in the domain name instead of the website's actual IP address. Risk factor : None OID : 1.3.6.1.4.1.25623.1.0.100069
Informational	unknown (49152/tcp)	Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this port: UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:163.26.17.1[49152] Solution : filter incoming traffic to this port. Risk factor : Low OID : 1.3.6.1.4.1.25623.1.0.10736
Informational	unknown (49153/tcp)	Distributed Computing Environment (DCE) services running on the remote host

		can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this port: UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:163.26.17.1[49153] Annotation: Event log TCPIP UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:163.26.17.1[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:163.26.17.1[49153] Annotation: DHCP Client LRPC Endpoint Solution : filter incoming traffic to this port. Risk factor : Low OID : 1.3.6.1.4.1.25623.1.0.10736
Informational	unknown (49154/tcp)	Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this port: UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:163.26.17.1[49154] UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:163.26.17.1[49154] Annotation: IKE/Authip API UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1 Endpoint: ncacn_ip_tcp:163.26.17.1[49154] UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:163.26.17.1[49154] Annotation: Impl friendly name Solution : filter incoming traffic to this port. Risk factor : Low OID : 1.3.6.1.4.1.25623.1.0.10736
Informational	unknown (49155/tcp)	Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this port: UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:163.26.17.1[49155] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access

		Solution : filter incoming traffic to this port. Risk factor : Low OID : 1.3.6.1.4.1.25623.1.0.10736
Informational	unknown (49156/tcp)	Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this port: UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5 Endpoint: ncacn_ip_tcp:163.26.17.1[49156] Named pipe : dnsserver Win32 service or process : dns.exe Description : DNS Server Solution : filter incoming traffic to this port. Risk factor : Low OID : 1.3.6.1.4.1.25623.1.0.10736
Informational	unknown (49162/tcp)	Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this port: UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:163.26.17.1[49162] Solution : filter incoming traffic to this port. Risk factor : Low OID : 1.3.6.1.4.1.25623.1.0.10736
Informational	general/SMBClient	OS Version = Windows Server (R) 2008 Enterprise 6002 Service Pack 2 Domain = WORKGROUP SMB Serverversion = Windows Server (R) 2008 Enterprise 6.0 OID : 1.3.6.1.4.1.25623.1.0.90011
Informational	general/SMBClient	OS Version = Windows Server (R) 2008 Enterprise 6002 Service Pack 2 Domain = WORKGROUP SMB Serverversion = WINDOWS SERVER (R) 2008 ENTERPRISE 6.0 OID : 1.3.6.1.4.1.25623.1.0.90011
Informational	general/SMBClient	OS Version = WINDOWS SERVER (R) 2008 ENTERPRISE 6002 SERVICE PACK 2 Domain = WORKGROUP SMB Serverversion = Windows Server (R) 2008 Enterprise 6.0 OID : 1.3.6.1.4.1.25623.1.0.90011
Informational	general/SMBClient	OS Version = WINDOWS SERVER (R) 2008 ENTERPRISE 6002 SERVICE PACK 2 Domain = WORKGROUP SMB Serverversion = WINDOWS SERVER (R) 2008 ENTERPRISE 6.0 OID : 1.3.6.1.4.1.25623.1.0.90011

This file was generated by the OpenVAS security scanner.