



OUTSCAN Security Report

Sections

[Report info >>](#)

[Executive summary - Security Overview >>](#)

[Host list summary >>](#)

[Open port list >>](#)

[Vulnerability details >>](#)

[Modification list >>](#)

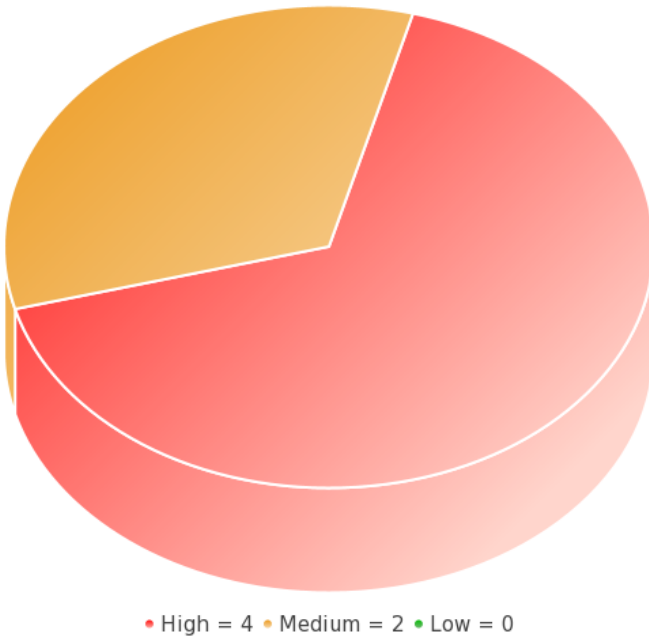
[Scan tracking list >>](#)

Report info

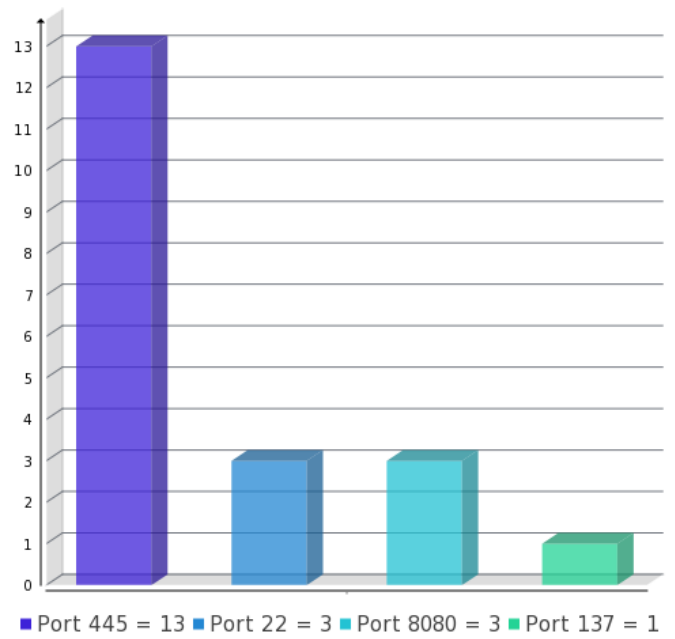
Report Type:	Detailed report
Report ID:	B59FA7D4E81D219CBA34FCA85FC5D565
Date Report was created:	2009-11-24 11:16
Timezone for dates:	GMT
Report created for:	Demo company
Schedule job:	Web servers
IPs:	intra.example.com - 192.168.200.45
Report Interval:	2009-11-04 10:00 - 2009-11-04 10:00
Number of Scans:	1
Number of Findings found:	23

Executive summary - Security Overview

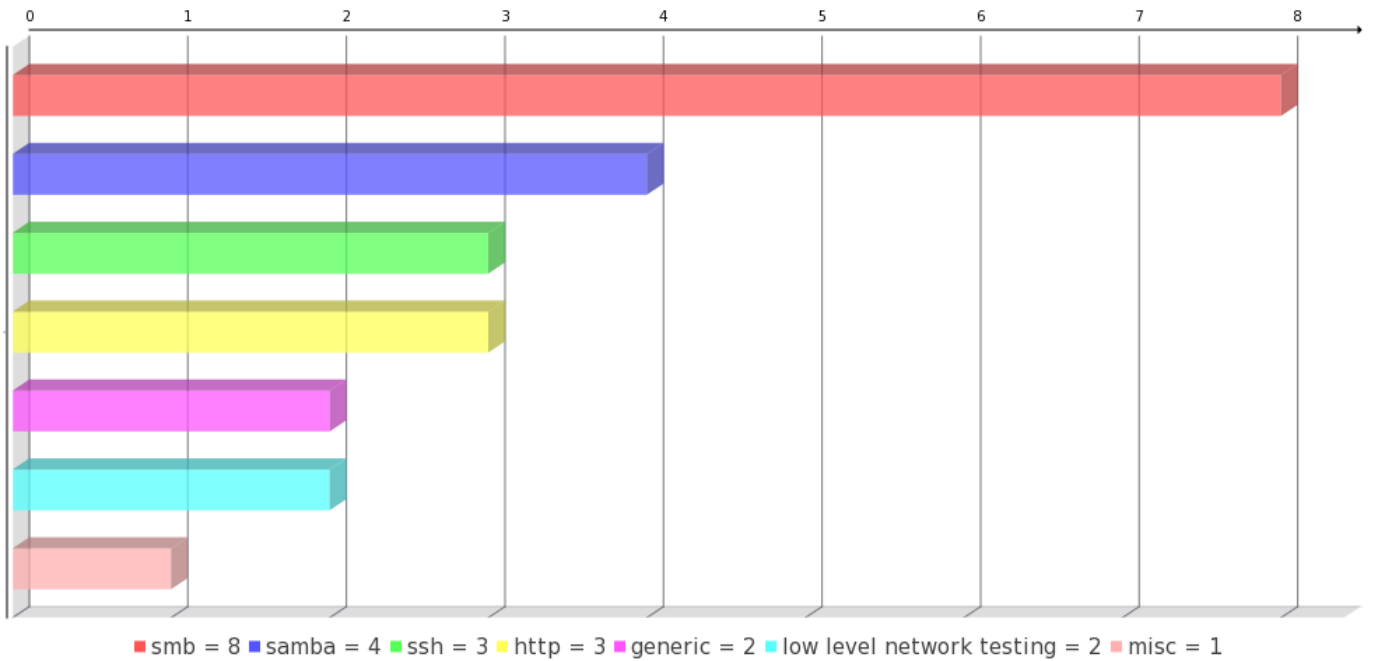
Risk Level Overview



Top Port Overview



Risk Category Overview



Host list summary

	High risk	Medium risk	Low risk	Information	Open ports
intra.example.com - 192.168.200.45	4	2	0	17	6
Scanning interval: 2009-11-04 11:00 - 2009-11-04 13:33 Template: Normal					

Open port list

intra.example.com 192.168.200.45 2009-11-04 11:00	22/tcp - ssh 137/udp - netbios-ns 139/tcp - netbios-ssn 445/tcp - netbios-ssn 8009/tcp - ajp 8080/tcp - http
--	---

Vulnerability details - 192.168.200.45 (intra.example.com)

Script ID:	219055
Name:	Samba: Filename-base Format String Bug
Port:	445/tcp - netbios-ssn
Risk factor:	High risk
CVSS Score:	9.3 - (AV:N/AC:M/Au:N/C:C/I:C/A:C) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	samba
Description:	Multiple format string vulnerabilities in client/client.c in smbclient in Samba 3.2.0 through 3.2.12 might allow context-dependent attackers to execute arbitrary code via format string specifiers in a filename.
Information:	This vulnerability was identified because (1) the version of Samba, 3.2.3, is less than or equal to 3.2.12.
Solution:	Upgrade to the latest version of Samba
CVE:	CVE-2009-1886
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	215073
Name:	Samba: smbdc *trans* Request Arbitrary Remote Memory Disclosure
Port:	445/tcp - netbios-ssn
Risk factor:	High risk
CVSS Score:	8.5 - (AV:N/AC:L/Au:N/C:C/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	samba

Description:	smbd in Samba might allow remote attackers to read arbitrary memory and cause a denial of service via crafted (1) trans, (2) trans2, and (3) ntrans requests, related to a "cut&paste error" that causes an improper bounds check to be performed.
Information:	This vulnerability was identified because (1) the version of Samba, 3.2.3, is greater than or equal to 3.0.29; and (2) the version of Samba, 3.2.3, is less than or equal to 3.2.4.
Solution:	Upgrade to the latest version of Samba
CVE:	CVE-2008-4314
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	110956
Name:	Anonymous SMB Login Enabled
Port:	445/tcp - netbios-ssn
Risk factor:	High risk
CVSS Score:	7.5 - (AV:N/AC:L/Au:N/C:P/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	generic
Description:	Anonymous access to this SMB service is enabled. If this is an internet-facing server, having anonymous access to it is generally a bad idea.
Solution:	Reconfigure this service.
Reference:	url - http://support.microsoft.com/kb/q143474/ url - http://support.microsoft.com/kb/q246261/
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	217926
Name:	SMB Null Sessions Enabled
Port:	445/tcp - netbios-ssn
Risk factor:	High risk
CVSS Score:	7.5 - (AV:N/AC:L/Au:N/C:P/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	generic
Description:	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet-facing server, having anonymous access to it is generally a bad idea.
Solution:	Reconfigure this service.
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	217011
-------------------	--------

Name:	Samba Root Filesystem Access Vulnerability
Port:	445/tcp - netbios-ssn
Risk factor:	Medium risk
CVSS Score:	6.3 - (AV:N/AC:M/Au:S/C:C/I:N/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	samba
Description:	Samba 3.2.0 through 3.2.6, when registry shares are enabled, allows remote authenticated users to access the root filesystem via a crafted connection request that specifies a blank share name.
Information:	This vulnerability was identified because (1) the version of Samba, 3.2.3, is greater than or equal to 3.2.0; and (2) the version of Samba, 3.2.3, is less than or equal to 3.2.6.
Solution:	Upgrade to the latest version of Samba
CVE:	CVE-2009-0022
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	219054
Name:	Samba: POSIX Access Control Override
Port:	445/tcp - netbios-ssn
Risk factor:	Medium risk
CVSS Score:	5.8 - (AV:N/AC:M/Au:N/C:P/I:P/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	samba
Description:	The acl_group_override function in smbd/posix_acls.c in smbd in Samba 3.0.x before 3.0.35, 3.1.x and 3.2.x before 3.2.13, and 3.3.x before 3.3.6, when dos filemode is enabled, allows remote attackers to modify access control lists for files via vectors related to read access to uninitialized memory.
Information:	This vulnerability was identified because (1) the version of Samba, 3.2.3, is less than or equal to 3.2.12.
Solution:	Upgrade to the latest version of Samba
CVE:	CVE-2009-1888
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	200217
Name:	ICMP Timestamp Request
Port:	General
Family:	low level network testing
Description:	The remote host replies to ICMP Timestamp requests. Knowing the exact time on your system may help an attacker to break time-based authentication systems.

Solution:	Filter incoming ICMP type 13, and outgoing ICMP type 14 packets.
CVE:	CVE-1999-0524
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	125901
Name:	SSH Supported Protocol Versions
Port:	22/tcp - ssh
Family:	ssh
Description:	The remote host is running a version of the SSH protocol. OUTSCAN has detected that the following is true for the remote host.
Information:	The SSH service appears to support the protocol version(s): 1.99, 2.0 Hostkey version 2: 33:8f:7c:a6:11:c0:25:5f:1f:f1:8b:ad:18:fb:09:84
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	200823
Name:	SSH Supported Authentication Mechanisms
Port:	22/tcp - ssh
Family:	ssh
Description:	The SSH service running on this port supports the following authentication mechanisms.
Information:	publickey,password
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	125993
Name:	Traceroute
Port:	General
Family:	misc
Description:	<p>This check tries to determine the path; traceroute, between our attacker and your target host. This path may give an attacker valuable information about through which routers; hops, traffic passes through. This is not a vulnerability in itself it is merely considered information, however, an attacker could possibly use this information to determine what ISP you have and so forth.</p> <p>Note: The path is not static and will most likely change depending on from which host you perform the traceroute. There is also no way you can fix this problem as it involves changing configurations on all the hops along the way.</p>

Information:	host[:dport]/protocol (1 hops) 1 192.168.200.45:53/udp [closed]
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	200275
Name:	SMB Host Security Identifier
Port:	445/tcp - netbios-ssn
Family:	smb
Description:	It was possible to get the host Security Identifier (SID) through the SMB service, by calling LsaQueryInformationPolicy. This can be used to enumerate local user accounts.
Information:	SID: 1-5-21-897084493--634054598--2011538493
Solution:	Restrict access to the SMB service
CVE:	CVE-2000-1200
Bugtraq:	959
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	125644
Name:	SMB Network Share Enumeration
Port:	445/tcp - netbios-ssn
Family:	smb
Description:	SMB shares available on this host:
Information:	<u>Share name</u> print\$ IPC\$
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	217925
Name:	SMB Login
Port:	445/tcp - netbios-ssn
Family:	smb
Description:	This check attempts to login to the remote SMB service.
Information:	The following login attempts were successful:

- Null session [<blank> / <blank>]
- Anonymous login [<random> / <random>]

Selected login type: Anonymous login

History: First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22

Target: intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID: 125677

Name: SMB Native LanMan Information

Port: 445/tcp - netbios-ssn

Family: smb

Description: Sending an authentication request to this host reveals the following information:

Information: Domain: UBUNTU810
Native LanMan: Samba 3.2.3
Operating System: Unix

History: First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22

Target: intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID: 113289

Name: NetBIOS Name Enumeration

Port: 137/udp - netbios-ns

Family: smb

Description: A NetBIOS service replies to queries on udp port 137.

Information: MAC address: 00:00:00:00:00:00 (Probably a SAMBA server)
NetBIOS names found:

<u>Name</u>	<u>Description</u>
UBUNTU810	computer name
UBUNTU810	messenger service
UBUNTU810	file server service
__MSBROWSE__	master browser
WORKGROUP	master browser
WORKGROUP	browser service elections
WORKGROUP	workgroup / domain name

CVE: CVE-1999-0621

History: First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22

Target: intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID: 124463

Name:	HTTP Detection
Port:	8080/tcp - http
Family:	http
Description:	An HTTP server was found running on the remote host.
Information:	Apache-Coyote/1.1
Virtual host:	192.168.200.45
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	125898
Name:	SSH Banner
Port:	22/tcp - ssh
Family:	ssh
Description:	The SSH server banner:
Information:	SSH-2.0-OpenSSH_5.1p1 Debian-3ubuntu1
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	125796
Name:	SMB Host Password Policy
Port:	445/tcp - netbios-ssn
Family:	smb
Description:	The remote host has a password policy set. This password policy must conform to the International System Policy.
Information:	Note: OUTSCAN used the supplied credentials to authenticate The remote host has the following password policy: Password history length: 0 Minimum password length: 5 Password aging: 0 days Password complexity requirements: Enabled Minimum password age: 0 days Forced logoff: Disabled Locked account after: 1800 seconds Time between failed logons: 1800 seconds
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	125665
Name:	SMB LanMan Pipe Server Browsing

Port:	445/tcp - netbios-ssn
Family:	smb
Description:	This host will reveal the list of other nearby Windows systems when queried through the LanMan pipe.
Information:	The following hosts were revealed: UBUNTU810 (os version: 0.0)
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	200276
Name:	SMB Host SID Local User Enumeration
Port:	445/tcp - netbios-ssn
Family:	smb
Description:	It was possible to enumerate the local users of the remote host. This could give an attacker valuable information.
Information:	The following accounts were found during the enumeration: Guest account name: nobody
CVE:	CVE-2000-1200
Bugtraq:	959
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	200825
Name:	HTTP Options
Port:	8080/tcp - http
Family:	http
Description:	The following options are allowed by the webserver running on this port.
Information:	GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
Virtual host:	192.168.200.45
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Script ID:	200826
Name:	HTTP Information
Port:	8080/tcp - http

Family:	http			
Description:	HTTP Server Information			
Information:	<u>HTTP Version</u> 1.1	<u>SSL</u> no	<u>Request Pipelining</u> yes	<u>Connection Keep-Alive</u> yes
Reference:	url - http://www.io.com/~maus/HttpKeepAlive.html url - http://www.mozilla.org/projects/netlib/http/pipelining-faq.html			
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22			
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00			

Script ID:	125950
Name:	TCP SYN FIN
Port:	General
Family:	low level network testing
Description:	<p>The TCP implementation on this host replies to invalid TCP packets. Packets with both the SYN and the FIN bit set are considered invalid and should be discarded.</p> <p>Not doing so could have a negative impact on IDS systems. Depending on the order in which the flag-bits are parsed, the TCP implementation of this host's operating system may see the SYN bit first and initiate a connection while the TCP implementation of the IDS parses the FIN bit first, making it believe that the connection has just been closed.</p> <p>Effectively, this could mean that a connection can be established without the IDS keeping track of it.</p>
Solution:	Contact your operating system vendor for a patch.
Reference:	url - http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html url - http://www.kb.cert.org/vuls/id/464113 url - http://nvd.nist.gov/nvd.cfm?cvename=CVE-2007-3537
Bugtraq:	7487
History:	First Seen : 2009-11-06 11:22 - Last Seen : 2009-11-06 11:22
Target:	intra.example.com - 192.168.200.45 - 2009-11-04 11:00

Modification list

None

Scan tracking list

intra.example.com 192.168.200.45