KPMC

Report generated by Nessus™ Wed, 06 Jun 2018 17:39:54 GMT+0100

TABLE OF CONTENTS

Hosts Executive Summary

Hosts Executive Summary

192.168.1.64

Vulnerabilities Total: 22

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10287	Traceroute Information
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	10919	Open Port Re-check
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	11936	OS Identification
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	22964	Service Detection
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	46180	Additional DNS Hostnames
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection

INFO	N/A	54615	Device Type
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)

192.168.1.77

Vulnerabilities Total: 48

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	11714	Nonexistent Page (404) Physical Path Disclosure
MEDIUM	5.0	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	10144	Microsoft SQL Server TCP/IP Listener Detection
INFO	N/A	10147	Nessus Server Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10674	Microsoft SQL Server UDP Query Remote Version Disclosure
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	11936	OS Identification

INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	12634	Authenticated Check : OS Name and Installed Package Enumeration
INFO	N/A	14272	Netstat Portscanner (SSH)
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	21745	Authentication Failure - Local Checks Not Run
INFO	N/A	22964	Service Detection
INFO	N/A	24242	Microsoft .NET Handlers Enumeration
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	46180	Additional DNS Hostnames
INFO	N/A	51891	SSL Session Resume Supported
INFO	N/A	54615	Device Type
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	58651	Netstat Active Connections
INFO	N/A	64582	Netstat Connection Information
INFO	N/A	69482	Microsoft SQL Server STARTTLS Support
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	85805	HTTP/2 Cleartext Detection

INFO	N/A	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	104743	TLS Version 1.0 Protocol Detection
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	108761	MSSQL Host Information in NTLM SSP

192.168.1.253

Vulnerabilities Total: 44

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	15985	Samba smbd Security Descriptor Parsing Remote Overflow
CRITICAL	10.0	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
HIGH	9.0	34769	Dropbear SSH Server svr_ses.childpidsize Remote Overflow
MEDIUM	6.8	90509	Samba Badlock Vulnerability
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	21023	Dropbear SSH Authorization-pending Connection Saturation DoS
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	10287	Traceroute Information
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	10919	Open Port Re-check
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	11026	Wireless Access Point Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	11936	OS Identification
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	22964	Service Detection
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	25240	Samba Server Detection
INFO	N/A	30207	LPD Detection
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	50845	OpenSSL Detection
INFO	N/A	54615	Device Type
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	66334	Patch Report
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	85805	HTTP/2 Cleartext Detection
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	104887	Samba Version

INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)

192.168.1.254

Vulnerabilities Total: 14

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.8	42263	Unencrypted Telnet Server
INFO	N/A	10281	Telnet Server Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	10919	Open Port Re-check
INFO	N/A	11002	DNS Server Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	11936	OS Identification
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	54615	Device Type
INFO	N/A	85805	HTTP/2 Cleartext Detection