My Basic Network Scan

Report generated by Nessus™ Fri, 28 Aug 2020 04:08:12 PDT

TABLE OF CONTENTS

Hosts Executive Summary

Hosts Executive Summary

192.168.247.144

1	2	25	6	72
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 106

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	58327	Samba 'AndX' Request Heap-Based Buffer Overflow
HIGH	7.5	41028	SNMP Agent Default Community Name (public)
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.8	77200	OpenSSL 'ChangeCipherSpec' MiTM Vulnerability
MEDIUM	6.8	90509	Samba Badlock Vulnerability
MEDIUM	6.4	43156	NTP ntpd Mode 7 Error Response Packet Loop Remote DoS
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.0	10677	Apache mod_status /server-status Information Disclosure
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	97861	Network Time Protocol (NTP) Mode 6 Scanner
MEDIUM	5.0	71783	Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS
MEDIUM	5.0	73412	OpenSSL Heartbeat Information Disclosure (Heartbleed)
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	76474	SNMP 'GETBULK' Reflection DDoS
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname

MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	88098	Apache Server ETag Header Information Disclosure
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.0	52611	SMTP Service STARTTLS Plaintext Command Injection
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	2.6	62565	Transport Layer Security (TLS) Protocol CRIME Vulnerability
LOW	2.6	10407	X Server Detection
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	84574	Backported Security Patch Detection (PHP)
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection

INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10092	FTP Server Detection
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	14274	Nessus SNMP Scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	50845	OpenSSL Detection
INFO	N/A	57323	OpenSSL Version Detection
INFO	N/A	48243	PHP Version Detection
INFO	N/A	66334	Patch Report
INFO	N/A	10263	SMTP Server Detection
INFO	N/A	35296	SNMP Protocol Version Detection
INFO	N/A	34022	SNMP Query Routing Information Disclosure

INFO	N/A	10550	SNMP Query Running Process List Disclosure
INFO	N/A	10800	SNMP Query System Information Disclosure
INFO	N/A	10551	SNMP Request Network Interfaces Enumeration
INFO	N/A	40448	SNMP Supported Protocols Detection
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	62563	SSL Compression Methods Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	51891	SSL Session Resume Supported
INFO	N/A	25240	Samba Server Detection
INFO	N/A	104887	Samba Version
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	87242	TLS NPN Supported Protocol Enumeration
INFO	N/A	62564	TLS Next Protocols Supported
INFO	N/A	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	136318	TLS Version 1.2 Protocol Detection

INFO	N/A	10287	Traceroute Information
INFO	N/A	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	19288	VNC Server Security Type Detection
INFO	N/A	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	10342	VNC Software Detection
INFO	N/A	135860	WMI Not Available
INFO	N/A	32318	Web Site Cross-Domain Policy File Detection
INFO	N/A	11424	WebDAV Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	106628	lighttpd HTTP Server Detection
INFO	N/A	66717	mDNS Detection (Local Network)
INFO	N/A	106375	nginx HTTP Server Detection