hands-on-basic-network

Report generated by Nessus™ Tue, 19 Jun 2018 12:03:49 CEST

TABLE OF CONTENTS

Hosts Executive Summary

192.168.17.1 4

192.168.17.10 6

192.168.17.21 7

192.168.17.31 12

192.168.17.41 15

192.168.17.53 17

192.168.17.252 22

192.168.17.253 24

192.168.17.254 26

Hosts Executive Summary

192.168.17.1

0	0	0	0	20
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

Total: 20

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	10287	Traceroute Information
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	11040	HTTP Reverse Proxy Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	11936	OS Identification
INFO	N/A	18261	Apache Banner Linux Distribution Disclosure
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	39520	Backported Security Patch Detection (SSH)
INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	54615	Device Type

INFO	N/A	70657	SSH Algorithms and Languages Supported

192.168.17.10

0	0	0	0	17
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 17

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	10287	Traceroute Information
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	11002	DNS Server 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	25220	TCP/IP Timestamps Supported
INFO	N/A	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	72779	DNS Server Version Detection

192.168.17.21

7	3	18	7	69
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 104

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	10203	rexecd Service Detection
CRITICAL	10.0	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0	51988	Bind Shell Backdoor Detection
CRITICAL	10.0	61708	VNC Server 'password' Password
HIGH	7.5	10205	rlogin Service Detection
HIGH	7.5	10245	rsh Service Detection
HIGH	7.5	34460	Unsupported Web Server Detection
MEDIUM	6.8	12085	Apache Tomcat Default Files
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	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	5.0	42256	NFS Shares World Readable

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	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3	57792	Apache HTTP Server httpOnly Cookie Information Disclosure
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.3	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.0	52611	SMTP Service STARTTLS Plaintext Command Injection
LOW	2.6	10407	X Server Detection
LOW	2.6	31705	SSL Anonymous Cipher Suites Supported
LOW	2.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
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	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
INFO	N/A	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	10092	FTP Server Detection
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	10223	RPC portmapper Service Detection
INFO	N/A	10263	SMTP Server Detection
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	10281	Telnet Server Detection

INFO	N/A	10287	Traceroute Information
INFO	N/A	10342	VNC Software Detection
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	10437	NFS Share Export List
INFO	N/A	10719	MySQL Server Detection
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	11002	DNS Server Detection
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	11040	HTTP Reverse Proxy Detection
INFO	N/A	11111	RPC Services Enumeration
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	11156	IRC Daemon Version Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	11936	OS Identification
INFO	N/A	17975	Service Detection (GET request)
INFO	N/A	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	19288	VNC Server Security Type Detection
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	21186	AJP Connector Detection

INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	22227	RMI Registry Detection
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	26024	PostgreSQL Server Detection
INFO	N/A	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	39446	Apache Tomcat Detection
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	42088	SMTP Service STARTTLS Command Support
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	48243	PHP Version Detection
INFO	N/A	50845	OpenSSL Detection
INFO	N/A	51891	SSL Session Resume Supported
INFO	N/A	52703	vsftpd Detection
INFO	N/A	53335	RPC portmapper (TCP)
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	62563	SSL Compression Methods Supported
INFO	N/A	65792	VNC Server Unencrypted Communication Detection

INFO	N/A	66334	Patch Report
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	84574	Backported Security Patch Detection (PHP)
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	104743	TLS Version 1.0 Protocol Detection
INFO	N/A	104887	Samba Version
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)

192.168.17.31

4	1	5	2	38
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 50

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	73182	Microsoft Windows XP Unsupported Installation Detection
CRITICAL	10.0	97994	Microsoft IIS 6.0 Unsupported Version Detection
CRITICAL	10.0	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
CRITICAL	10.0	108797	Unsupported Windows OS
HIGH	7.5	34460	Unsupported Web Server Detection
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	26920	Microsoft Windows SMB NULL Session Authentication
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
LOW	2.6	54582	SMTP Service Cleartext Login Permitted
INFO	N/A	10077	Microsoft FrontPage Extensions Check
INFO	N/A	10092	FTP Server Detection
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	10263	SMTP Server Detection
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	10695	Microsoft IIS .IDA ISAPI Filter Enabled
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	10940	Windows Terminal Services Enabled
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	11040	HTTP Reverse Proxy Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	11874	Microsoft IIS 404 Response Service Pack Signature
INFO	N/A	11936	OS Identification
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	22319	MSRPC Service Detection
INFO	N/A	22964	Service Detection
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	31422	Reverse NAT/Intercepting Proxy Detection
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	54580	SMTP Authentication Methods

INFO	N/A	54615	Device Type
INFO	N/A	66173	RDP Screenshot
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	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	108659	SMTP Host Information in NTLM SSP
INFO	N/A	108804	Microsoft Exchange Server Detection (Uncredentialed)

192.168.17.41

3	0	5	1	27
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 36

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	84729	Microsoft Windows Server 2003 Unsupported Installation Detection
CRITICAL	10.0	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
CRITICAL	10.0	108797	Unsupported Windows OS
MEDIUM	6.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	26920	Microsoft Windows SMB NULL Session Authentication
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
INFO	N/A	10092	FTP Server Detection
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	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	10940	Windows Terminal Services Enabled

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	19506	Nessus Scan Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	22319	MSRPC Service Detection
INFO	N/A	22964	Service Detection
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	31422	Reverse NAT/Intercepting Proxy Detection
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	66173	RDP Screenshot
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	106716	Microsoft Windows SMB2 Dialects Supported (remote check)

192.168.17.53

2	1	24	8	69
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 104

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	10203	rexecd Service Detection
CRITICAL	10.0	58327	Samba 'AndX' Request Heap-Based Buffer Overflow
HIGH	7.5	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.8	77200	OpenSSL 'ChangeCipherSpec' MiTM Vulnerability
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	10677	Apache mod_status /server-status Information Disclosure
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	12218	mDNS Detection (Remote Network)
MEDIUM	5.0	15901	SSL Certificate Expiry
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	5.0	71783	Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS
MEDIUM	5.0	73412	OpenSSL Heartbeat Information Disclosure (Heartbleed)
MEDIUM	5.0	76474	SNMP 'GETBULK' Reflection DDoS

MEDIUM	5.0	88098	Apache Server ETag Header Information Disclosure
MEDIUM	5.0	97861	Network Time Protocol (NTP) Mode 6 Scanner
MEDIUM	4.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3	62565	Transport Layer Security (TLS) Protocol CRIME Vulnerability
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.3	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.0	52611	SMTP Service STARTTLS Plaintext Command Injection
LOW	2.6	10407	X Server Detection
LOW	2.6	31705	SSL Anonymous Cipher Suites Supported
LOW	2.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
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	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	10092	FTP Server Detection
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	10263	SMTP Server Detection
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	10287	Traceroute Information
INFO	N/A	10342	VNC Software Detection
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	10550	SNMP Query Running Process List Disclosure
INFO	N/A	10551	SNMP Request Network Interfaces Enumeration
INFO	N/A	10719	MySQL Server Detection
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	10800	SNMP Query System Information Disclosure
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	11040	HTTP Reverse Proxy Detection
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	11424	WebDAV Detection
INFO	N/A	11936	OS Identification
INFO	N/A	14274	Nessus SNMP Scanner
INFO	N/A	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	19288	VNC Server Security Type Detection
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	21643	SSL Cipher Suites Supported
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	32318	Web Site Cross-Domain Policy File Detection
INFO	N/A	34022	SNMP Query Routing Information Disclosure
INFO	N/A	35296	SNMP Protocol Version Detection
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	40448	SNMP Supported Protocols Detection
INFO	N/A	42088	SMTP Service STARTTLS Command Support
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	48204	Apache HTTP Server Version
INFO	N/A	48243	PHP Version Detection
INFO	N/A	50845	OpenSSL Detection
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	57323	OpenSSL Version Detection
INFO	N/A	62563	SSL Compression Methods Supported
INFO	N/A	62564	TLS Next Protocols Supported
INFO	N/A	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	66334	Patch Report
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	70657	SSH Algorithms and Languages Supported

INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	84574	Backported Security Patch Detection (PHP)
INFO	N/A	87242	TLS NPN Supported Protocol Enumeration
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	104743	TLS Version 1.0 Protocol Detection
INFO	N/A	104887	Samba Version
INFO	N/A	106375	nginx HTTP Server Detection
INFO	N/A	106628	lighttpd HTTP Server Detection
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)

192.168.17.252

0	0	3	0	35
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 38

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	97861	Network Time Protocol (NTP) Mode 6 Scanner
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10192	HTTP Proxy CONNECT Request Relaying
INFO	N/A	10195	HTTP Proxy Open Relay Detection
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	10287	Traceroute Information
INFO	N/A	10386	Web Server No 404 Error Code Check
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	11040	HTTP Reverse Proxy Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	11936	OS Identification
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	21643	SSL Cipher Suites Supported
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	39520	Backported Security Patch Detection (SSH)
INFO	N/A	42822	Strict Transport Security (STS) Detection
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	49692	Squid Proxy Version Detection
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	62564	TLS Next Protocols Supported
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	87242	TLS NPN Supported Protocol Enumeration
INFO	N/A	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	106198	pfSense Web Interface Detection
INFO	N/A	106375	nginx HTTP Server Detection
INFO	N/A	106658	JQuery Detection
INFO	N/A	106952	pfSense Detection

192.168.17.253

0	0	2	0	23
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 25

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10287	Traceroute Information
INFO	N/A	10386	Web Server No 404 Error Code Check
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	11040	HTTP Reverse Proxy Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	11936	OS Identification
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	21643	SSL Cipher Suites Supported
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	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	62564	TLS Next Protocols Supported
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	106375	nginx HTTP Server Detection

192.168.17.254

0	0	3	0	32
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 35

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	97861	Network Time Protocol (NTP) Mode 6 Scanner
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	10287	Traceroute Information
INFO	N/A	10386	Web Server No 404 Error Code Check
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	11040	HTTP Reverse Proxy Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	11936	OS Identification
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	21643	SSL Cipher Suites Supported
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	39520	Backported Security Patch Detection (SSH)
INFO	N/A	42822	Strict Transport Security (STS) Detection
INFO	N/A	45590	Common Platform Enumeration (CPE)
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	62564	TLS Next Protocols Supported
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	87242	TLS NPN Supported Protocol Enumeration
INFO	N/A	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	106198	pfSense Web Interface Detection
INFO	N/A	106375	nginx HTTP Server Detection
INFO	N/A	106658	JQuery Detection
INFO	N/A	106952	pfSense Detection