Location B – credentials

Report generated by Nessus™

Wed, 27 Mar 2024 15:31:48 CET

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.0.1

0	0	1	4	33
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

Total: 38

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	4.9	50686	IP Forwarding Enabled
LOW	3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.3*	-	10663	DHCP Server Detection
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	91634	HyperText Transfer Protocol (HTTP) Redirect Information
INFO	N/A	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

INFO	N/A	-	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	21745	OS Security Patch Assessment Failed
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	31422	Reverse NAT/Intercepting Proxy Detection
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	104410	Target Credential Status by Authentication Protocol - Failure for Provided Credentials
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	87872	Unbound DNS Resolver Remote Version Detection
INFO	N/A	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	91815	Web Application Sitemap
INFO	N/A	-	10662	Web mirroring

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.0.100

0	0	4	0	47
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

Total: 51

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	15901	SSL Certificate Expiry
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	42255	NFS Server Superfluous
INFO	N/A	-	10223	RPC portmapper Service Detection
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	-	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	-	91634	HyperText Transfer Protocol (HTTP) Redirect Information
INFO	N/A	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
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	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	42823	Non-compliant Strict Transport Security (STS)
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	21745	OS Security Patch Assessment Failed
INFO	N/A	-	122364	Python Remote HTTP Detection
INFO	N/A	-	11111	RPC Services Enumeration
INFO	N/A	-	53335	RPC portmapper (TCP)
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	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	87242	TLS NPN Supported Protocol Enumeration
INFO	N/A	-	62564	TLS Next Protocols Supported
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection

INFO	N/A	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	104410	Target Credential Status by Authentication Protocol - Failure for Provided Credentials
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	91815	Web Application Sitemap
INFO	N/A	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	66717	mDNS Detection (Local Network)
INFO	N/A	-	106375	nginx HTTP Server Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.0.101

0	0	0	0	4
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 4

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	11933	Do not scan printers
INFO	N/A	-	14274	Nessus SNMP Scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.0.105

0	1	1	0	27
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

Total: 29

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	7.5*	6.6	42411	Microsoft Windows SMB Shares Unprivileged Access
MEDIUM	5.3	-	57608	SMB Signing not required
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	-	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	23974	Microsoft Windows SMB Share Hosting Office Files
INFO	N/A	-	10395	Microsoft Windows SMB Shares Enumeration
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	-	11219	Nessus SYN scanner

INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	21745	OS Security Patch Assessment Failed
INFO	N/A	-	35705	SMB Registry : Starting the Registry Service during the scan failed
INFO	N/A	-	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	150799	Target Access Problems by Authentication Protocol - Maximum Privilege Account Used in Scan
INFO	N/A	-	141118	Target Credential Status by Authentication Protocol - Valid Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.0.106

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	0	43

Vulnerabilities Total: 44

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
INFO	N/A	-	12634	Authenticated Check : OS Name and Installed Package Enumeration
INFO	N/A	-	34098	BIOS Info (SSH)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	55472	Device Hostname
INFO	N/A	-	54615	Device Type
INFO	N/A	-	25203	Enumerate IPv4 Interfaces via SSH
INFO	N/A	-	25202	Enumerate IPv6 Interfaces via SSH
INFO	N/A	-	33276	Enumerate MAC Addresses via SSH
INFO	N/A	-	170170	Enumerate the Network Interface configuration via SSH
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10147	Nessus Server Detection

INFO	N/A	-	64582	Netstat Connection Information
INFO	N/A	-	14272	Netstat Portscanner (SSH)
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	-	110695	OS Security Patch Assessment Checks Not Supported
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	45405	Reachable IPv6 address
INFO	N/A	-	25221	Remote listeners enumeration (Linux / AIX)
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	56468	Time of Last System Startup
INFO	N/A	-	91815	Web Application Sitemap
INFO	N/A	-	11032	Web Server Directory Enumeration

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.0.111

0	0	0	0	21
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 21

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	14788	IP Protocols Scan
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	21745	OS Security Patch Assessment Failed
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported

INFO	N/A	-	104410	Target Credential Status by Authentication Protocol - Failure for Provided Credentials
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.0.112

0	0	0	0	20
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

Total: 20

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	21745	OS Security Patch Assessment Failed
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported

INFO	N/A	-	104410	Target Credential Status by Authentication Protocol - Failure for Provided Credentials
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.8.1

0	0	3	0	29
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 32

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	40406	CGI Generic Tests HTTP Errors
INFO	N/A	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	69826	HTTP Cookie 'secure' Property Transport Mismatch
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	56984	SSL / TLS Versions Supported
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	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps 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	-	85602	Web Application Cookies Not Marked Secure
INFO	N/A	-	91815	Web Application Sitemap
INFO	N/A	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	10662	Web mirroring

* indicates the v3.0 score was not available; the v2.0 score is shown