Nessus Report

Nessus Scan Report

Thu, 07 Dec 2017 21:35:58 EET

Table Of Contents

Hosts Summary (Executive)

10.99.0.21

Summary

Critical	High	Medium	Low	Info	Total
0	0	7	3	39	49

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported
Medium (5.0)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Medium (4.3)	85582	Web Application Potentially Vulnerable to Clickjacking
Medium (4.3)	90317	SSH Weak Algorithms Supported
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
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
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10223	RPC portmapper Service Detection
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10386	Web Server No 404 Error Code Check
Info	10662	Web mirroring
Info	10863	SSL Certificate Information
Info	10881	SSH Protocol Versions Supported
Info	10884	Network Time Protocol (NTP) Server Detection
Info	11111	RPC Services Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported

Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	39520	Backported Security Patch Detection (SSH)
Info	40665	Protected Web Page Detection
Info	42057	Web Server Allows Password Auto-Completion
Info	42822	Strict Transport Security (STS) Detection
Info	45590	Common Platform Enumeration (CPE)
Info	49704	External URLs
Info	50344	Missing or Permissive Content-Security-Policy HTTP Response Header
Info	50345	Missing or Permissive X-Frame-Options HTTP Response Header
Info	50845	OpenSSL Detection
Info	51080	Web Server Uses Basic Authentication over HTTPS
Info	53335	RPC portmapper (TCP)
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	70657	SSH Algorithms and Languages Supported
Info	85601	Web Application Cookies Not Marked HttpOnly
Info	91634	HyperText Transfer Protocol (HTTP) Redirect Information
Info	91815	Web Application Sitemap

10.99.0.100

Summary

Critical	High	Medium	Low	Info	Total
0	0	9	2	25	36

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported
Medium (5.0)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	80035	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Medium (4.0)	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	10736	DCE Services Enumeration
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	21745	Authentication Failure - Local Checks Not Run
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported

Info	35716	Ethernet Card Manufacturer Detection
Info	42981	SSL Certificate Expiry - Future Expiry
Info	45410	SSL Certificate 'commonName' Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	83298	SSL Certificate Chain Contains Certificates Expiring Soon
Info	84502	HSTS Missing From HTTPS Server

10.99.0.101

Summary

Critical	High	Medium	Low	Info	Total
0	0	9	2	26	37

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported
Medium (5.0)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	80035	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Medium (4.0)	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10736	DCE Services Enumeration
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	21745	Authentication Failure - Local Checks Not Run
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information

Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	42981	SSL Certificate Expiry - Future Expiry
Info	45410	SSL Certificate 'commonName' Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	83298	SSL Certificate Chain Contains Certificates Expiring Soon
Info	84502	HSTS Missing From HTTPS Server

10.99.0.102

Summary

Critical	High	Medium	Low	Info	Total
1	0	10	3	25	39

Details

Severity	Plugin Id	Name
Critical (10.0)	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (5.0)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	80035	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Medium (4.0)	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
Low (2.6)	10407	X Server Detection
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	21745	Authentication Failure - Local Checks Not Run
Info	22964	Service Detection

Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	42981	SSL Certificate Expiry - Future Expiry
Info	45410	SSL Certificate 'commonName' Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	83298	SSL Certificate Chain Contains Certificates Expiring Soon
Info	84502	HSTS Missing From HTTPS Server

10.99.0.103

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	3	3

Details

Severity	Plugin Id	Name
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	35716	Ethernet Card Manufacturer Detection

10.99.0.104

Summary

Critical	High	Medium	Low	Info	Total
0	0	9	2	25	36

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported
Medium (5.0)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	80035	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Medium (4.0)	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	10736	DCE Services Enumeration
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	21745	Authentication Failure - Local Checks Not Run
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported

Info	35716	Ethernet Card Manufacturer Detection
Info	42981	SSL Certificate Expiry - Future Expiry
Info	45410	SSL Certificate 'commonName' Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	83298	SSL Certificate Chain Contains Certificates Expiring Soon
Info	84502	HSTS Missing From HTTPS Server

10.99.0.105

Summary

Critical	High	Medium	Low	Info	Total
1	0	10	2	25	38

Details

Severity	Plugin Id	Name
Critical (10.0)	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (5.0)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	80035	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Medium (4.0)	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	21745	Authentication Failure - Local Checks Not Run
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information

Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	42981	SSL Certificate Expiry - Future Expiry
Info	45410	SSL Certificate 'commonName' Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	83298	SSL Certificate Chain Contains Certificates Expiring Soon
Info	84502	HSTS Missing From HTTPS Server

10.99.0.106

Summary

Critical	High	Medium	Low	Info	Total
0	0	9	3	22	34

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported
Medium (5.0)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	80035	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Medium (4.0)	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
Low (2.6)	10407	X Server Detection
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	21745	Authentication Failure - Local Checks Not Run
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection

Info	42981	SSL Certificate Expiry - Future Expiry
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	83298	SSL Certificate Chain Contains Certificates Expiring Soon
Info	84502	HSTS Missing From HTTPS Server

10.99.0.107

Summary

Critical	High	Medium	Low	Info	Total
0	0	9	2	22	33

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported
Medium (5.0)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	80035	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Medium (4.0)	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	21745	Authentication Failure - Local Checks Not Run
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	42981	SSL Certificate Expiry - Future Expiry

Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	83298	SSL Certificate Chain Contains Certificates Expiring Soon
Info	84502	HSTS Missing From HTTPS Server

10.99.0.108

Summary

Critical	High	Medium	Low	Info	Total
0	0	9	2	22	33

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported
Medium (5.0)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	80035	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Medium (4.0)	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	21745	Authentication Failure - Local Checks Not Run
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	42981	SSL Certificate Expiry - Future Expiry

Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	83298	SSL Certificate Chain Contains Certificates Expiring Soon
Info	84502	HSTS Missing From HTTPS Server

10.99.0.109

Summary

Critical	High	Medium	Low	Info	Total
2	0	11	2	34	49

Details

Severity	Plugin Id	Name
Critical (10.0)	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
Critical (10.0)	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
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 Disabled
Medium (5.0)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	80035	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Medium (4.0)	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10863	SSL Certificate Information
Info	11011	Microsoft Windows SMB Service Detection

Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	21745	Authentication Failure - Local Checks Not Run
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35716	Ethernet Card Manufacturer Detection
Info	42981	SSL Certificate Expiry - Future Expiry
Info	45410	SSL Certificate 'commonName' Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	83298	SSL Certificate Chain Contains Certificates Expiring Soon
Info	84502	HSTS Missing From HTTPS Server
Info	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
Info	100871	Microsoft Windows SMB Versions Supported (remote check)
Info	104410	Host Authentication Failure(s) for Provided Credentials

10.99.0.110

Summary

Critical	High	Medium	Low	Info	Total
10	144	32	2	94	282

Details

Severity	Plugin Id	Name
Critical (10.0)	22024	Microsoft Internet Explorer Unsupported Version Detection
Critical (10.0)	26921	Windows Service Pack Out-of-Date
Critical (10.0)	44422	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468)
Critical (10.0)	48291	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)
Critical (10.0)	53377	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)
Critical (10.0)	56736	MS11-083: Vulnerability in TCP/IP Could Allow Remote Code Execution (2588516)
Critical (10.0)	61529	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)
Critical (10.0)	63419	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)
Critical (10.0)	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
Critical (10.0)	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
High (9.3)	42110	MS09-054: Cumulative Security Update for Internet Explorer (974455)
High (9.3)	43064	MS09-072: Cumulative Security Update for Internet Explorer (976325)
High (9.3)	43865	MS10-001: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (972270)
High (9.3)	44110	MS10-002: Cumulative Security Update for Internet Explorer (978207)
High (9.3)	44416	MS10-006: Vulnerabilities in SMB Client Could Allow Remote Code Execution (978251)
High (9.3)	44423	MS10-013: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (977935)
High (9.3)	45378	MS10-018: Cumulative Security Update for Internet Explorer (980182)
High (9.3)	45506	MS10-019: Vulnerabilities in Windows Could Allow Remote Code Execution (981210)
High (9.3)	45507	MS10-020: Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)

High (9.3)	46312	MS10-030: Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution (978542)
High (9.3)	46840	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution (979902)
High (9.3)	46842	MS10-035: Cumulative Security Update for Internet Explorer (982381)
High (9.3)	47711	MS10-043: Vulnerability in Canonical Display Driver Could Allow Remote Code Execution (2032276)
High (9.3)	47750	MS KB2286198: Windows Shell Shortcut Icon Parsing Arbitrary Code Execution (EASYHOOKUP)
High (9.3)	48216	MS10-046: Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198) (EASYHOOKUP)
High (9.3)	48286	MS10-049: Vulnerabilities in SChannel could allow Remote Code Execution (980436)
High (9.3)	48288	MS10-051: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2079403)
High (9.3)	48290	MS10-053: Cumulative Security Update for Internet Explorer (2183461)
High (9.3)	48297	MS10-060: Vulnerabilities in the Microsoft .NET Common Language Runtime and in Microsoft Silverlight Could Allow Remote Code Execution (2265906)
High (9.3)	48762	MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution
High (9.3)	49219	MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) (EMERALDTHREAD)
High (9.3)	49948	MS10-071: Cumulative Security Update for Internet Explorer (2360131)
High (9.3)	49951	MS10-074: Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution (2387149)
High (9.3)	49953	MS10-076: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (982132)
High (9.3)	49960	MS10-083: Vulnerability in COM Validation in Windows Shell and WordPad Could Allow Remote Code Execution (2405882)
High (9.3)	51162	MS10-090: Cumulative Security Update for Internet Explorer (2416400)
High (9.3)	51163	MS10-091: Vulnerabilities in the OpenType Font (OTF) Driver Could Allow Remote Code Execution (2296199)
High (9.3)	51167	MS10-095: Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2385678)
High (9.3)	51168	MS10-096: Vulnerability in Windows Address Book Could Allow Remote Code Execution (2423089)
High (9.3)	51455	MS11-002: Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution (2451910)
High (9.3)	51587	MS KB2488013: Internet Explorer CSS Import Rule Processing Arbitrary Code Execution

High (9.3)	51903	MS11-003: Cumulative Security Update for Internet Explorer (2482017)
High (9.3)	51907	MS11-007: Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2485376)
High (9.3)	52585	MS11-017: Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution (2508062)
High (9.3)	53375	MS11-018: Cumulative Security Update for Internet Explorer (2497640)
High (9.3)	53376	MS11-019: Vulnerabilities in SMB Client Could Allow Remote Code Execution (2511455)
High (9.3)	53382	MS11-025: Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Remote Code Execution (2500212)
High (9.3)	53385	MS11-028: Vulnerability in .NET Framework Could Allow Remote Code Execution (2484015)
High (9.3)	53388	MS11-031: Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution (2514666)
High (9.3)	53389	MS11-032: Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2507618)
High (9.3)	55118	MS11-038: Vulnerability in OLE Automation Could Allow Remote Code Execution (2476490)
High (9.3)	55119	MS11-039: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2514842)
High (9.3)	55121	MS11-041: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2525694)
High (9.3)	55122	MS11-042: Vulnerabilities in Distributed File System Could Allow Remote Code Execution (2535512)
High (9.3)	55124	MS11-044: Vulnerability in .NET Framework Could Allow Remote Code Execution (2538814)
High (9.3)	55130	MS11-050: Cumulative Security Update for Internet Explorer (2530548)
High (9.3)	55132	MS11-052: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (2544521)
High (9.3)	55787	MS11-057: Critical Cumulative Security Update for Internet Explorer (2559049)
High (9.3)	56174	MS11-071: Vulnerability in Windows Components Could Allow Remote Code Execution (2570947)
High (9.3)	56449	MS11-075: Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution (2623699)
High (9.3)	56451	MS11-077: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2567053)
High (9.3)	56452	MS11-078: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2604930)
High (9.3)	56455	MS11-081: Critical Cumulative Security Update for Internet Explorer (2586448)

High (9.3)	56738	MS11-085: Vulnerability in Windows Mail and Windows Meeting Space Could Allow Remote Code Execution (2620704)
High (9.3)	57273	MS11-087: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2639417)
High (9.3)	57276	MS11-090: Cumulative Security Update of ActiveX Kill Bits (2618451)
High (9.3)	57285	MS11-099: Cumulative Security Update for Internet Explorer (2618444)
High (9.3)	57414	MS11-100: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2638420)
High (9.3)	57469	MS12-001: Vulnerability in Windows Kernel Could Allow Security Feature Bypass (2644615)
High (9.3)	57472	MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution (2636391)
High (9.3)	57473	MS12-005: Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2584146)
High (9.3)	57942	MS12-008: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)
High (9.3)	57944	MS12-010: Cumulative Security Update for Internet Explorer (2647516)
High (9.3)	57946	MS12-012: Vulnerability in Color Control Panel Could Allow Remote Code Execution (2643719)
High (9.3)	57947	MS12-013: Vulnerability in C Run-Time Library Could Allow Remote Code Execution (2654428)
High (9.3)	57950	MS12-016: Vulnerabilities in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2651026)
High (9.3)	58332	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)
High (9.3)	58655	MS12-023: Cumulative Security Update for Internet Explorer (2675157)
High (9.3)	58656	MS12-024: Vulnerability in Windows Could Allow Remote Code Execution (2653956)
High (9.3)	58657	MS12-025: Vulnerability in .NET Framework Could Allow Remote Code Execution (2671605)
High (9.3)	59042	MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)
High (9.3)	59043	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2693777)
High (9.3)	59044	MS 2695962: Update Rollup for ActiveX Kill Bits (2695962)
High (9.3)	59454	MS12-036: Vulnerability in Remote Desktop Could Allow Remote Code Execution (2685939)
High (9.3)	59455	MS12-037: Cumulative Security Update for Internet Explorer (2699988)
High (9.3)	59456	MS12-038: Vulnerability in .NET Framework Could Allow Remote Code Execution (2706726)

High (9.3)	59906	MS12-043: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2722479)
High (9.3)	59908	MS12-045: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (2698365)
High (9.3)	59911	MS12-048: Vulnerability in Windows Shell Could Allow Remote Code Execution (2691442)
High (9.3)	61527	MS12-052: Cumulative Security Update for Internet Explorer (2722913)
High (9.3)	61531	MS12-056: Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution (2706045)
High (9.3)	62045	MS 2736233: Update Rollup for ActiveX Kill Bits (2736233)
High (9.3)	62223	MS12-063: Cumulative Security Update for Internet Explorer (2744842)
High (9.3)	62906	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2745030)
High (9.3)	62907	MS12-075: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2761226)
High (9.3)	63224	MS12-077: Cumulative Security Update for Internet Explorer (2761465)
High (9.3)	63225	MS12-078: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2783534)
High (9.3)	63228	MS12-081: Vulnerability in Windows File Handling Component Could Allow Remote Code Execution (2758857)
High (9.3)	63229	MS12-082: Vulnerability in DirectPlay Could Allow Remote Code Execution (2770660)
High (9.3)	63420	MS13-002: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (2756145)
High (9.3)	63422	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2769324)
High (9.3)	63522	MS13-008: Security Update for Internet Explorer (2799329)
High (9.3)	64570	MS13-009: Security Update for Internet Explorer (2792100)
High (9.3)	64571	MS13-010: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (2797052)
High (9.3)	64576	MS13-015: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2800277)
High (9.3)	65210	MS13-021: Security Update for Internet Explorer (2809289)
High (9.3)	65875	MS13-028: Security Update for Internet Explorer (2817183)
High (9.3)	65876	MS13-029: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution (2828223)
High (9.3)	91230	7-Zip < 16.00 Multiple Vulnerabilities
High (8.5)	59459	MS12-041: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2709162)

High (7.8)	42115	MS09-059: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (975467)
High (7.8)	55128	MS11-048: Vulnerability in SMB Server Could Allow Denial of Service (2536275)
High (7.8)	55286	MS11-048: Vulnerability in SMB Server Could Allow Denial of Service (2536275) (remote check)
High (7.8)	55794	MS11-064: Vulnerabilities in TCP/IP Stack Could Allow Denial of Service (2563894)
High (7.8)	64579	MS13-018: Vulnerability in TCP/IP Could Allow Denial of Service (2790655)
High (7.6)	45509	MS10-022: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (981169)
High (7.6)	49958	MS10-081: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2296011)
High (7.6)	53381	MS11-024: Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution (2527308)
High (7.6)	55123	MS11-043: Vulnerability in SMB Client Could Allow Remote Code Execution (2536276)
High (7.6)	56824	MS KB2506014: Update for the Windows Operating System Loader
High (7.6)	103876	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)
High (7.5)	53387	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553)
High (7.2)	46839	MS10-032: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (979559)
High (7.2)	48284	MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852)
High (7.2)	48285	MS10-048: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329)
High (7.2)	48295	MS10-058: Vulnerabilities in TCP/IP Could Allow Elevation of Privilege (978886)
High (7.2)	48296	MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799)
High (7.2)	49950	MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957)
High (7.2)	51164	MS10-092: Vulnerability in Task Scheduler Could Allow Elevation of Privilege (2305420)
High (7.2)	51170	MS10-098: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)
High (7.2)	51172	MS10-100: Vulnerability in Consent User Interface Could Allow Elevation of Privilege (2442962)
High (7.2)	51911	MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802)

High (7.2)	51912	MS11-012: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2479628)
High (7.2)	51913	MS11-013: Vulnerabilities in Kerberos Could Allow Elevation of Privilege (2496930)
High (7.2)	53391	MS11-034: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2506223)
High (7.2)	55126	MS11-046: Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2503665)
High (7.2)	55570	MS11-054: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2555917)
High (7.2)	55793	MS11-063: Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2567680)
High (7.2)	57283	MS11-097: Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2620712)
High (7.2)	57943	MS12-009: Vulnerabilities in Ancillary Function Driver Could Allow Elevation of Privilege (2645640)
High (7.2)	59460	MS12-042: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2711167)
High (7.2)	59910	MS12-047: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2718523)
High (7.2)	61530	MS12-055: Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2731847)
High (7.2)	62463	MS12-068: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2724197)
High (7.2)	63423	MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930)
High (7.2)	64577	MS13-016: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778344)
High (7.2)	64578	MS13-017: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2799494)
High (7.2)	64580	MS13-019: Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege (2790113)
High (7.2)	65215	MS13-027: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege (2807986)
High (7.2)	65878	MS13-031: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2813170)
High (7.2)	65883	MS13-036: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2829996)
High (7.1)	49962	MS10-085: Vulnerability in SChannel Could Allow Denial of Service (2207566)
High (7.1)	55798	MS11-068: Vulnerability in Windows Kernel Could Allow Denial of Service (2556532)

High (7.1)	56737	MS11-084: Vulnerability in Windows Kernel-Mode Drivers Could Allow Denial of Service (2617657)
Medium (6.9)	46844	MS10-037: Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Elevation of Privilege (980218)
Medium (6.9)	59040	MS12-032: Vulnerability in TCP/IP Could Allow Elevation of Privilege (2688338)
Medium (6.9)	59041	MS12-033: Vulnerability in Windows Partition Manager Could Allow Elevation of Privilege (2690533)
Medium (6.8)	48761	MS KB982316: Elevation of Privilege Using Windows Service Isolation Bypass
Medium (6.6)	58330	MS12-018: Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2641653)
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	55799	MS11-069: Vulnerability in .NET Framework Could Allow Information Disclosure (2567951)
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (6.4)	63230	MS12-083: Vulnerability in IP-HTTPS Component Could Allow Security Feature Bypass (2765809)
Medium (6.2)	45508	MS10-021: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)
Medium (6.2)	55572	MS11-056: Vulnerabilities in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2507938)
Medium (5.8)	62466	MS KB2661254: Update For Minimum Certificate Key Length
Medium (5.8)	63424	MS13-006: Vulnerability in Microsoft Windows Could Allow Security Feature Bypass (2785220)
Medium (5.1)	44418	MS10-008: Cumulative Security Update of ActiveX Kill Bits (978262)
Medium (5.1)	46841	MS10-034: Cumulative Security Update of ActiveX Kill Bits (980195)
Medium (5.1)	53384	MS11-027: Cumulative Security Update of ActiveX Kill Bits (2508272)
Medium (5.1)	55802	MS 2562937: Update Rollup for ActiveX Kill Bits (2562937)
Medium (5.1)	58335	MS 2647518: Update Rollup for ActiveX Kill Bits (2647518)
Medium (5.0)	42112	MS09-056: Vulnerabilities in Windows CryptoAPI Could Allow Spoofing (974571)
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (5.0)	46848	MS10-041: Vulnerability in Microsoft .NET Framework Could Allow Tampering (981343)
Medium (5.0)	49695	MS10-070: Vulnerability in ASP.NET Could Allow Information Disclosure (2418042)
Medium (5.0)	57608	SMB Signing Disabled

Medium (5.0)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Medium (4.3)	51909	MS11-009: Vulnerability in JScript and VBScript Scripting Engine Could Allow Information Disclosure (2475792)
Medium (4.3)	53383	MS11-026: Vulnerability in MHTML Could Allow Information Disclosure (2503658)
Medium (4.3)	55117	MS11-037: Vulnerability in MHTML Could Allow Information Disclosure (2544893)
Medium (4.3)	57474	MS12-006: Vulnerability in SSL/TLS Could Allow Information Disclosure (2643584)
Medium (4.3)	59912	MS12-049: Vulnerability in TLS Could Allow Information Disclosure (2655992)
Medium (4.3)	62464	MS12-069: Vulnerability in Kerberos Could Allow Denial of Service (2743555)
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Low (2.6)	11457	Microsoft Windows SMB Registry : Winlogon Cached Password Weakness
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10396	Microsoft Windows SMB Shares Access
Info	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
Info	10399	SMB Use Domain SID to Enumerate Users
Info	10400	Microsoft Windows SMB Registry Remotely Accessible
Info	10456	Microsoft Windows SMB Service Enumeration
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Info	10860	SMB Use Host SID to Enumerate Local Users
Info	10863	SSL Certificate Information
Info	10897	Microsoft Windows - Users Information : Disabled Accounts
Info	10898	Microsoft Windows - Users Information : Never Changed Password
Info	10899	Microsoft Windows - Users Information : User Has Never Logged In

Info	10902	Microsoft Windows 'Administrators' Group User List
Info	10913	Microsoft Windows - Local Users Information : Disabled Accounts
Info	10914	Microsoft Windows - Local Users Information : Never Changed Passwords
Info	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
Info	10919	Open Port Re-check
Info	10940	Windows Terminal Services Enabled
Info	11011	Microsoft Windows SMB Service Detection
Info	11032	Web Server Directory Enumeration
Info	11936	OS Identification
Info	17651	Microsoft Windows SMB : Obtains the Password Policy
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	20811	Microsoft Windows Installed Software Enumeration (credentialed check)
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	24269	Windows Management Instrumentation (WMI) Available
Info	24270	Computer Manufacturer Information (WMI)
Info	24272	Network Interfaces Enumeration (WMI)
Info	34096	BIOS Version (WMI)
Info	34220	Netstat Portscanner (WMI)
Info	34252	Microsoft Windows Remote Listeners Enumeration (WMI)
Info	35716	Ethernet Card Manufacturer Detection
Info	38153	Microsoft Windows Summary of Missing Patches
Info	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
Info	42822	Strict Transport Security (STS) Detection
Info	42823	Non-compliant Strict Transport Security (STS)
Info	43111	HTTP Methods Allowed (per directory)
Info	44401	Microsoft Windows SMB Service Config Enumeration
Info	45410	SSL Certificate 'commonName' Mismatch
Info	45590	Common Platform Enumeration (CPE)

Info	46180	Additional DNS Hostnames
Info	48337	Windows ComputerSystemProduct Enumeration (WMI)
Info	48942	Microsoft Windows SMB Registry : OS Version and Processor Architecture
Info	49704	External URLs
Info	50344	Missing or Permissive Content-Security-Policy HTTP Response Header
Info	50345	Missing or Permissive X-Frame-Options HTTP Response Header
Info	51351	Microsoft .NET Framework Detection
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	55472	Device Hostname
Info	56310	Firewall Rule Enumeration
Info	56468	Time of Last System Startup
Info	56954	Microsoft Revoked Digital Certificates Enumeration
Info	56984	SSL / TLS Versions Supported
Info	57033	Microsoft Patch Bulletin Feasibility Check
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	58181	Windows DNS Server Enumeration
Info	58452	Microsoft Windows Startup Software Enumeration
Info	58651	Netstat Active Connections
Info	63080	Microsoft Windows Mounted Devices
Info	63620	Windows Product Key Retrieval
Info	64582	Netstat Connection Information
Info	64814	Terminal Services Use SSL/TLS
Info	66334	Patch Report
Info	70329	Microsoft Windows Process Information
Info	70331	Microsoft Windows Process Module Information
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	71246	Enumerate Local Group Memberships
Info	72367	Microsoft Internet Explorer Version Detection
Info	72482	Windows Display Driver Enumeration
Info	72684	Enumerate Local Users

Info	72879	Microsoft Internet Explorer Enhanced Security Configuration Detection
Info	91231	7-Zip Installed
Info	91815	Web Application Sitemap
Info	92365	Microsoft Windows Hosts File
Info	92367	Microsoft Windows PowerShell Execution Policy
Info	92371	Microsoft Windows DNS Cache
Info	92421	Internet Explorer Typed URLs
Info	92424	MUICache Program Execution History
Info	92428	Recent File History
Info	92431	User Shell Folders Settings
Info	92434	User Download Folder Files
Info	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
Info	97086	Server Message Block (SMB) Protocol Version 1 Enabled
Info	100871	Microsoft Windows SMB Versions Supported (remote check)
Info	103871	Microsoft Windows Network Adapters

10.99.0.111

Summary

Critical	High	Medium	Low	Info	Total
1	0	10	2	25	38

Details

Severity	Plugin Id	Name
Critical (10.0)	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (5.0)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	80035	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Medium (4.0)	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	21745	Authentication Failure - Local Checks Not Run
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information

Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	42981	SSL Certificate Expiry - Future Expiry
Info	45410	SSL Certificate 'commonName' Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	83298	SSL Certificate Chain Contains Certificates Expiring Soon
Info	84502	HSTS Missing From HTTPS Server

10.99.0.120

Summary

Critical	High	Medium	Low	Info	Total
1	0	4	0	23	28

Details

Severity	Plugin Id	Name
Critical (10.0)	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10736	DCE Services Enumeration
Info	10863	SSL Certificate Information
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	45410	SSL Certificate 'commonName' Mismatch
Info	50845	OpenSSL Detection
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

Info	94761	SSL Root Certification Authority Certificate Information
Info	104410	Host Authentication Failure(s) for Provided Credentials

10.99.0.130

Summary

Critical	High	Medium	Low	Info	Total
0	0	3	2	27	32

Details

Severity	Plugin Id	Name
Medium (5.0)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (5.0)	46803	PHP expose_php Information Disclosure
Medium (4.3)	90317	SSH Weak Algorithms Supported
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10881	SSH Protocol Versions Supported
Info	11032	Web Server Directory Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	39520	Backported Security Patch Detection (SSH)
Info	39521	Backported Security Patch Detection (WWW)
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version Detection
Info	49704	External URLs

Info	50344	Missing or Permissive Content-Security-Policy HTTP Response Header
Info	50345	Missing or Permissive X-Frame-Options HTTP Response Header
Info	54615	Device Type
Info	70657	SSH Algorithms and Languages Supported
Info	84574	Backported Security Patch Detection (PHP)
Info	91815	Web Application Sitemap

10.99.0.222

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	8	8

Details

Severity	Plugin Id	Name
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	11819	TFTP Daemon Detection
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	35716	Ethernet Card Manufacturer Detection
Info	66717	mDNS Detection (Local Network)

10.99.0.234

Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	38	39

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Info	10107	HTTP Server Type and Version
Info	10147	Nessus Server Detection
Info	10267	SSH Server Type and Version Information
Info	10863	SSL Certificate Information
Info	10881	SSH Protocol Versions Supported
Info	11032	Web Server Directory Enumeration
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	12634	Authenticated Check : OS Name and Installed Package Enumeration
Info	14272	Netstat Portscanner (SSH)
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	21745	Authentication Failure - Local Checks Not Run
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25202	Enumerate IPv6 Interfaces via SSH
Info	25203	Enumerate IPv4 Interfaces via SSH
Info	25221	Remote listeners enumeration (Linux / AIX)
Info	33276	Enumerate MAC Addresses via SSH
Info	34098	BIOS version (SSH)
Info	35351	System Information Enumeration (via DMI)
Info	35716	Ethernet Card Manufacturer Detection
Info	45432	Processor Information (via DMI)
Info	45433	Memory Information (via DMI)

Info	45590	Common Platform Enumeration (CPE)
Info	50344	Missing or Permissive Content-Security-Policy HTTP Response Header
Info	54615	Device Type
Info	55472	Device Hostname
Info	56468	Time of Last System Startup
Info	56984	SSL / TLS Versions Supported
Info	58651	Netstat Active Connections
Info	64582	Netstat Connection Information
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	70657	SSH Algorithms and Languages Supported
Info	84502	HSTS Missing From HTTPS Server
Info	91815	Web Application Sitemap
Info	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

10.99.0.237

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	5	5

Details

Severity	Plugin Id	Name
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	35716	Ethernet Card Manufacturer Detection

10.99.0.251

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	17	17

Details

Severity	Plugin Id	Name
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10881	SSH Protocol Versions Supported
Info	11219	Nessus SYN scanner
Info	11819	TFTP Daemon Detection
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	39520	Backported Security Patch Detection (SSH)
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type
Info	66717	mDNS Detection (Local Network)
Info	70657	SSH Algorithms and Languages Supported