

# Nessus Report

Nessus Scan Report

Sat, 26 Mar 2016 23:04:20 EASST

# Table Of Contents

Hosts Summary (Executive).....	5
•10.1.62.0.....	6
•10.1.62.1.....	7
•10.1.62.2.....	8
•10.1.62.3.....	10
•10.1.62.4.....	11
•10.1.62.5.....	12
•10.1.62.6.....	14
•10.1.62.7.....	15
•10.1.62.8.....	17
•10.1.62.9.....	18
•10.1.62.10.....	19
•10.1.62.11.....	20
•10.1.62.12.....	21
•10.1.62.13.....	22
•10.1.62.14.....	23
•10.1.62.15.....	25
•10.1.62.16.....	26
•10.1.62.17.....	27
•10.1.62.18.....	28
•10.1.62.19.....	29
•10.1.62.20.....	30
•10.1.62.21.....	31
•10.1.62.22.....	32
•10.1.62.23.....	33
•10.1.62.24.....	34
•10.1.62.25.....	35
•10.1.62.26.....	36
•10.1.62.27.....	37
•10.1.62.28.....	38
•10.1.62.29.....	39
•10.1.62.30.....	40
•10.1.62.31.....	41
•10.1.62.32.....	42
•10.1.62.33.....	43
•10.1.62.34.....	44
•10.1.62.35.....	45
•10.1.62.36.....	46
•10.1.62.37.....	47
•10.1.62.38.....	48
•10.1.62.39.....	49
•10.1.62.40.....	50
•10.1.62.41.....	51
•10.1.62.42.....	52

●10.1.62.43.....	53
●10.1.62.44.....	54
●10.1.62.45.....	55
●10.1.62.46.....	56
●10.1.62.47.....	57
●10.1.62.48.....	58
●10.1.62.49.....	59
●10.1.62.50.....	60
●10.1.62.51.....	64
●10.1.62.52.....	65
●10.1.62.53.....	66
●10.1.62.54.....	67
●10.1.62.55.....	68
●10.1.62.56.....	70
●10.1.62.57.....	71
●10.1.62.58.....	72
●10.1.62.59.....	73
●10.1.62.60.....	74
●10.1.62.61.....	77
●10.1.62.62.....	78
●10.1.62.63.....	79
●10.1.62.64.....	80
●10.1.62.65.....	81
●10.1.62.66.....	82
●10.1.62.67.....	83
●10.1.62.68.....	84
●10.1.62.69.....	85
●10.1.62.70.....	86
●10.1.62.71.....	87
●10.1.62.72.....	88
●10.1.62.73.....	89
●10.1.62.74.....	90
●10.1.62.75.....	91
●10.1.62.76.....	92
●10.1.62.77.....	93
●10.1.62.78.....	94
●10.1.62.79.....	95
●10.1.62.80.....	96
●10.1.62.81.....	97
●10.1.62.82.....	98
●10.1.62.83.....	99
●10.1.62.84.....	100
●10.1.62.85.....	101
●10.1.62.86.....	102
●10.1.62.87.....	103
●10.1.62.88.....	104
●10.1.62.89.....	105

•10.1.62.90.....	106
•10.1.62.91.....	107
•10.1.62.92.....	108
•10.1.62.93.....	109
•10.1.62.94.....	110
•10.1.62.95.....	111
•10.1.62.96.....	112
•10.1.62.97.....	113
•10.1.62.98.....	114
•10.1.62.99.....	115
•10.1.62.100.....	116

## Hosts Summary (Executive)

10.1.62.0					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.1					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	11	11
Details					
Severity	Plugin Id	Name			
Info	10114	ICMP Timestamp Request Remote Date Disclosure			
Info	10180	Ping the remote host			
Info	10287	Traceroute Information			
Info	10919	Open Port Re-check			
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	35716	Ethernet Card Manufacturer Detection			
Info	66717	mDNS Detection (Local Network)			

### 10.1.62.2

#### Summary

Critical	High	Medium	Low	Info	Total
0	0	2	0	29	31

#### Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Info	10107	HTTP Server Type and Version
Info	10147	Nessus Server Detection
Info	10180	Ping the remote host
Info	10863	SSL Certificate Information
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	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	33276	Enumerate MAC Addresses via SSH
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	46215	Inconsistent Hostname and IP Address
Info	50845	OpenSSL Detection
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	84502	HSTS Missing From HTTPS Server

10.1.62.3					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.4					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.5					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	2	0	32	34
Details					
Severity	Plugin Id	Name			
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted			
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	10147	Nessus Server Detection			
Info	10180	Ping the remote host			
Info	10223	RPC portmapper Service Detection			
Info	10267	SSH Server Type and Version Information			
Info	10287	Traceroute Information			
Info	10863	SSL Certificate Information			
Info	10881	SSH Protocol Versions Supported			
Info	10919	Open Port Re-check			
Info	11032	Web Server Directory Enumeration			
Info	11111	RPC Services Enumeration			
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	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	45590	Common Platform Enumeration (CPE)			

Info	50845	OpenSSL Detection
Info	53335	RPC portmapper (TCP)
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	66717	mDNS Detection (Local Network)
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	70657	SSH Algorithms and Languages Supported
Info	84502	HSTS Missing From HTTPS Server

10.1.62.6					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	11	11
Details					
Severity	Plugin Id	Name			
Info	10114	ICMP Timestamp Request Remote Date Disclosure			
Info	10180	Ping the remote host			
Info	10287	Traceroute Information			
Info	10919	Open Port Re-check			
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	35716	Ethernet Card Manufacturer Detection			
Info	66717	mDNS Detection (Local Network)			

### 10.1.62.7

#### Summary

Critical	High	Medium	Low	Info	Total
0	0	2	0	25	27

#### Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
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	10147	Nessus Server Detection
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	10919	Open Port Re-check
Info	11032	Web Server Directory Enumeration
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	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	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	66717	mDNS Detection (Local Network)
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported





10.1.62.8					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	11	11
Details					
Severity	Plugin Id	Name			
Info	10114	ICMP Timestamp Request Remote Date Disclosure			
Info	10180	Ping the remote host			
Info	10287	Traceroute Information			
Info	10919	Open Port Re-check			
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	35716	Ethernet Card Manufacturer Detection			
Info	66717	mDNS Detection (Local Network)			

10.1.62.9					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.10					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.11					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

**10.1.62.12****Summary**

Critical	High	Medium	Low	Info	Total
0	0	0	0	14	14

**Details**

Severity	Plugin Id	Name
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10180	Ping the remote host
Info	10223	RPC portmapper Service Detection
Info	10287	Traceroute Information
Info	10919	Open Port Re-check
Info	11111	RPC Services Enumeration
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	35716	Ethernet Card Manufacturer Detection
Info	53335	RPC portmapper (TCP)
Info	66717	mDNS Detection (Local Network)

10.1.62.13					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

## 10.1.62.14

### Summary

Critical	High	Medium	Low	Info	Total
0	0	2	0	25	27

### Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
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	10147	Nessus Server Detection
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	10919	Open Port Re-check
Info	11032	Web Server Directory Enumeration
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	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	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	66717	mDNS Detection (Local Network)
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported





10.1.62.15					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.16					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.17					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.18					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.19					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

**10.1.62.20****Summary**

Critical	High	Medium	Low	Info	Total
0	0	0	0	13	13

**Details**

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
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	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

**10.1.62.21****Summary**

Critical	High	Medium	Low	Info	Total
0	0	0	0	13	13

**Details**

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
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	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

**10.1.62.22****Summary**

Critical	High	Medium	Low	Info	Total
0	0	0	0	13	13

**Details**

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
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	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type



**10.1.62.23****Summary**

Critical	High	Medium	Low	Info	Total
0	0	0	0	13	13

**Details**

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
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	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

**10.1.62.24****Summary**

Critical	High	Medium	Low	Info	Total
0	0	0	0	13	13

**Details**

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
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	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

10.1.62.25					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.26					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	13	13
Details					
Severity	Plugin Id	Name			
Info	10107	HTTP Server Type and Version			
Info	10180	Ping the remote host			
Info	10287	Traceroute Information			
Info	11219	Nessus SYN scanner			
Info	11936	OS Identification			
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	45590	Common Platform Enumeration (CPE)			
Info	54615	Device Type			

**10.1.62.27****Summary**

Critical	High	Medium	Low	Info	Total
0	0	0	0	13	13

**Details**

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
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	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

**10.1.62.28****Summary**

Critical	High	Medium	Low	Info	Total
0	0	0	0	13	13

**Details**

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
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	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

**10.1.62.29****Summary**

Critical	High	Medium	Low	Info	Total
0	0	0	0	13	13

**Details**

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
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	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

10.1.62.30					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			



10.1.62.31					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	13	13
Details					
Severity	Plugin Id	Name			
Info	10107	HTTP Server Type and Version			
Info	10180	Ping the remote host			
Info	10287	Traceroute Information			
Info	11219	Nessus SYN scanner			
Info	11936	OS Identification			
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	45590	Common Platform Enumeration (CPE)			
Info	54615	Device Type			

**10.1.62.32****Summary**

Critical	High	Medium	Low	Info	Total
0	0	0	0	13	13

**Details**

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
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	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

**10.1.62.33****Summary**

Critical	High	Medium	Low	Info	Total
0	0	0	0	13	13

**Details**

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
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	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

10.1.62.34					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.35					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.36					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.37					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.38					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			



10.1.62.39					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.40					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.41					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.42					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.43					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.44					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.45					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.46					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			



10.1.62.47					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.48					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.49					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

## 10.1.62.50

### Summary

Critical	High	Medium	Low	Info	Total
19	5	14	2	44	84

### Details

Severity	Plugin Id	Name
Critical (10.0)	10537	Microsoft IIS Unicode Remote Command Execution
Critical (10.0)	10657	MS01-023: Microsoft IIS 5.0 Malformed HTTP Printer Request Header Remote Buffer Overflow (953155) (uncredentialed check)
Critical (10.0)	11808	MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncredentialed check)
Critical (10.0)	11835	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed check)
Critical (10.0)	11890	MS03-043: Buffer Overrun in Messenger Service (828035) (uncredentialed check)
Critical (10.0)	12054	MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028) (uncredentialed check) (NTLM)
Critical (10.0)	12065	ASN.1 Multiple Integer Overflows (SMTP check)
Critical (10.0)	12209	MS04-011: Security Update for Microsoft Windows (835732) (uncredentialed check)
Critical (10.0)	13852	MS04-022: Microsoft Windows Task Scheduler Remote Overflow (841873) (uncredentialed check)
Critical (10.0)	18502	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)
Critical (10.0)	19407	MS05-043: Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) (uncredentialed check)
Critical (10.0)	19408	MS05-039: Vulnerability in Plug and Play Service Could Allow Remote Code Execution (899588) (uncredentialed check)
Critical (10.0)	20008	MS05-051: Vulnerabilities in MSDTC Could Allow Remote Code Execution (902400) (uncredentialed check)
Critical (10.0)	21193	MS05-047: Plug and Play Remote Code Execution and Local Privilege Elevation (905749) (uncredentialed check)
Critical (10.0)	21334	MS06-018: Vulnerability in Microsoft Distributed Transaction Coordinator Could Allow DoS (913580) (uncredentialed check)
Critical (10.0)	21655	MS04-012: Cumulative Update for Microsoft RPC/DCOM (828741) (uncredentialed check)
Critical (10.0)	22194	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)
Critical (10.0)	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
Critical (10.0)	47709	Microsoft Windows 2000 Unsupported Installation Detection

High (7.5)	10671	MS01-026 / MS01-044: Microsoft IIS Remote Command Execution (uncredentialed check)
High (7.5)	10703	Microsoft Windows SMTP Incorrect Credentials Authentication Bypass
High (7.5)	11110	MS02-045: Microsoft Windows SMB Protocol SMB_COM_TRANSACTION Packet Remote Overflow DoS (326830) (uncredentialed check)
High (7.5)	22034	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)
High (7.5)	34460	Unsupported Web Server Detection
Medium (6.4)	11308	Microsoft Windows SMTP Service NTLM Null Session Authorization Bypass (uncredentialed check)
Medium (5.0)	10079	Anonymous FTP Enabled
Medium (5.0)	10491	Microsoft IIS Translate f: ASP/ASA Source Disclosure
Medium (5.0)	10492	MS00-006: Microsoft IIS IDA/IDQ Multiple Vulnerabilities (uncredentialed check)
Medium (5.0)	10885	Microsoft Windows SMTP Service Malformed BDAT Request Remote DoS
Medium (5.0)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (5.0)	18585	Microsoft Windows SMB Service Enumeration via \srvsvc
Medium (5.0)	18602	Microsoft Windows SMB svcctl MSRPC Interface SCM Service Enumeration
Medium (5.0)	26920	Microsoft Windows SMB NULL Session Authentication
Medium (5.0)	56210	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials
Medium (5.0)	56211	SMB Use Host SID to Enumerate Local Users Without Credentials
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	10815	Web Server Generic XSS
Medium (4.3)	10936	Microsoft IIS Multiple Vulnerabilities (MS02-018)
Low (2.6)	34324	FTP Supports Cleartext Authentication
Low (2.6)	54582	SMTP Service Cleartext Login Permitted
Info	10077	Microsoft FrontPage Extensions Check
Info	10092	FTP Server Detection
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	10180	Ping the remote host
Info	10263	SMTP Server Detection

Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10661	Microsoft IIS 5 .printer ISAPI Filter Enabled
Info	10695	Microsoft IIS .IDA ISAPI Filter Enabled
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	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 on
Info	10916	Microsoft Windows - Local Users Information : Passwords never expire
Info	11011	Microsoft Windows SMB Service Detection
Info	11032	Web Server Directory Enumeration
Info	11219	Nessus SYN scanner
Info	11424	WebDAV Detection
Info	11874	Microsoft IIS 404 Response Service Pack Signature
Info	11936	OS Identification
Info	17651	Microsoft Windows SMB : Obtains the Password Policy
Info	17975	Service Detection (GET request)
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	22319	MSRPC Service Detection
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	24269	Windows Management Instrumentation (WMI) Available
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	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	54580	SMTP Authentication Methods
Info	54615	Device Type
Info	66334	Patch Report

10.1.62.51					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			



10.1.62.52					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.53					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.54					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

## 10.1.62.55

### Summary

Critical	High	Medium	Low	Info	Total
8	1	2	0	20	31

### Details

Severity	Plugin Id	Name
Critical (10.0)	11808	MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncredentialed check)
Critical (10.0)	11835	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed check)
Critical (10.0)	12054	MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028) (uncredentialed check) (NTLM)
Critical (10.0)	12209	MS04-011: Security Update for Microsoft Windows (835732) (uncredentialed check)
Critical (10.0)	22194	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)
Critical (10.0)	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)
Critical (10.0)	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
Critical (10.0)	84729	Microsoft Windows Server 2003 Unsupported Installation Detection
High (7.5)	22034	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)
Medium (5.0)	26920	Microsoft Windows SMB NULL Session Authentication
Medium (5.0)	57608	SMB Signing Disabled
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
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	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	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

10.1.62.56					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.57					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.58					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			



10.1.62.59					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

## 10.1.62.60

### Summary

Critical	High	Medium	Low	Info	Total
9	3	14	2	50	78

### Details

Severity	Plugin Id	Name
Critical (10.0)	11808	MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncredentialed check)
Critical (10.0)	11835	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed check)
Critical (10.0)	12054	MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028) (uncredentialed check) (NTLM)
Critical (10.0)	12209	MS04-011: Security Update for Microsoft Windows (835732) (uncredentialed check)
Critical (10.0)	22194	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)
Critical (10.0)	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)
Critical (10.0)	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
Critical (10.0)	71458	Nessus Unsupported Version Detection
Critical (10.0)	84729	Microsoft Windows Server 2003 Unsupported Installation Detection
High (9.4)	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
High (9.3)	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
High (7.5)	22034	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	26920	Microsoft Windows SMB NULL Session Authentication
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (5.0)	56210	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials
Medium (5.0)	56211	SMB Use Host SID to Enumerate Local Users Without Credentials

Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Medium (4.3)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	85582	Web Application Potentially Vulnerable to Clickjacking
Medium (4.3)	86949	Nessus 5.x < 5.2.12 / 6.x < 6.4 Multiple OpenSSL Vulnerabilities
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10147	Nessus Server Detection
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
Info	10399	SMB Use Domain SID to Enumerate Users
Info	10662	Web mirroring
Info	10736	DCE Services Enumeration
Info	10761	COM+ Internet Services (CIS) Server Detection
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	10884	Network Time Protocol (NTP) Server Detection
Info	10940	Windows Terminal Services Enabled
Info	11002	DNS Server Detection
Info	11011	Microsoft Windows SMB Service Detection
Info	11032	Web Server Directory Enumeration

Info	11219	Nessus SYN scanner
Info	11874	Microsoft IIS 404 Response Service Pack Signature
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	20870	LDAP Server Detection
Info	21643	SSL Cipher Suites Supported
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	25701	LDAP Crafted Search Request Server Information Disclosure
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35716	Ethernet Card Manufacturer Detection
Info	43111	HTTP Methods Allowed (per directory)
Info	43829	Kerberos Information Disclosure
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	49704	External URLs
Info	50845	OpenSSL Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	66173	RDP Screenshot
Info	66334	Patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	84502	HSTS Missing From HTTPS Server
Info	86067	SSL Certificate Signed Using SHA-1 Algorithm

10.1.62.61					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.62					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.63					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.64					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			



10.1.62.65					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.66					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.67					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.68					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.69					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.70					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.71					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.72					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			



10.1.62.73					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.74					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.75					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.76					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.77					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.78					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.79					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.80					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			



10.1.62.81					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.82					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.83					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.84					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.85					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.86					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.87					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.88					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			



10.1.62.89					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.90					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.91					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.92					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.93					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.94					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.95					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.96					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			



10.1.62.97					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.98					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.99					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			

10.1.62.100					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1
Details					
Severity	Plugin Id	Name			
Info	10180	Ping the remote host			