



# My Basic Network Scan

---

Report generated by Nessus™

Sun, 30 Jul 2023 22:01:47 Central Standard Time

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 10.0.0.1.....	4
• 10.0.0.10.....	7
• 10.0.0.39.....	10
• 10.0.0.40.....	11
• 10.0.0.41.....	12
• 10.0.0.42.....	13
• 10.0.0.46.....	14
• 10.0.0.47.....	16
• 10.0.0.51.....	17
• 10.0.0.55.....	19

---

## **Vulnerabilities by Host**

---

## 10.0.0.1



### Vulnerabilities

Total: 44

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	4.0	50686	IP Forwarding Enabled
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
LOW	3.3*	-	10663	DHCP Server Detection
LOW	3.3*	4.2	11197	Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	72779	DNS Server Version Detection
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version

INFO	N/A	-	<a href="#">24260</a>	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	<a href="#">11219</a>	Nessus SYN scanner
INFO	N/A	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	<a href="#">10884</a>	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	<a href="#">11936</a>	OS Identification
INFO	N/A	-	<a href="#">117886</a>	OS Security Patch Assessment Not Available
INFO	N/A	-	<a href="#">50845</a>	OpenSSL Detection
INFO	N/A	-	<a href="#">70657</a>	SSH Algorithms and Languages Supported
INFO	N/A	-	<a href="#">149334</a>	SSH Password Authentication Accepted
INFO	N/A	-	<a href="#">10881</a>	SSH Protocol Versions Supported
INFO	N/A	-	<a href="#">153588</a>	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	<a href="#">10267</a>	SSH Server Type and Version Information
INFO	N/A	-	<a href="#">56984</a>	SSL / TLS Versions Supported
INFO	N/A	-	<a href="#">10863</a>	SSL Certificate Information
INFO	N/A	-	<a href="#">70544</a>	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	<a href="#">21643</a>	SSL Cipher Suites Supported
INFO	N/A	-	<a href="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	<a href="#">156899</a>	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	<a href="#">22964</a>	Service Detection
INFO	N/A	-	<a href="#">25220</a>	TCP/IP Timestamps Supported
INFO	N/A	-	<a href="#">84821</a>	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	<a href="#">121010</a>	TLS Version 1.1 Protocol Detection
INFO	N/A	-	<a href="#">136318</a>	TLS Version 1.2 Protocol Detection
INFO	N/A	-	<a href="#">110723</a>	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	<a href="#">10287</a>	Traceroute Information

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

## 10.0.0.10



### Vulnerabilities

Total: 43

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	2.5	18405	Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	5.3	-	57608	SMB Signing not required
INFO	N/A	-	46180	Additional DNS Hostnames
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	-	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	60119	Microsoft Windows SMB Share Permissions Enumeration
INFO	N/A	-	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)

INFO	N/A	-	<a href="#">106716</a>	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	<a href="#">11219</a>	Nessus SYN scanner
INFO	N/A	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	<a href="#">11936</a>	OS Identification
INFO	N/A	-	<a href="#">117886</a>	OS Security Patch Assessment Not Available
INFO	N/A	-	<a href="#">10860</a>	SMB Use Host SID to Enumerate Local Users
INFO	N/A	-	<a href="#">70657</a>	SSH Algorithms and Languages Supported
INFO	N/A	-	<a href="#">149334</a>	SSH Password Authentication Accepted
INFO	N/A	-	<a href="#">10881</a>	SSH Protocol Versions Supported
INFO	N/A	-	<a href="#">153588</a>	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	<a href="#">10267</a>	SSH Server Type and Version Information
INFO	N/A	-	<a href="#">56984</a>	SSL / TLS Versions Supported
INFO	N/A	-	<a href="#">10863</a>	SSL Certificate Information
INFO	N/A	-	<a href="#">70544</a>	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	<a href="#">21643</a>	SSL Cipher Suites Supported
INFO	N/A	-	<a href="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	<a href="#">156899</a>	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	<a href="#">25240</a>	Samba Server Detection
INFO	N/A	-	<a href="#">22964</a>	Service Detection
INFO	N/A	-	<a href="#">25220</a>	TCP/IP Timestamps Supported
INFO	N/A	-	<a href="#">136318</a>	TLS Version 1.2 Protocol Detection
INFO	N/A	-	<a href="#">110723</a>	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	<a href="#">10287</a>	Traceroute Information
INFO	N/A	-	<a href="#">135860</a>	WMI Not Available



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

## 10.0.0.39



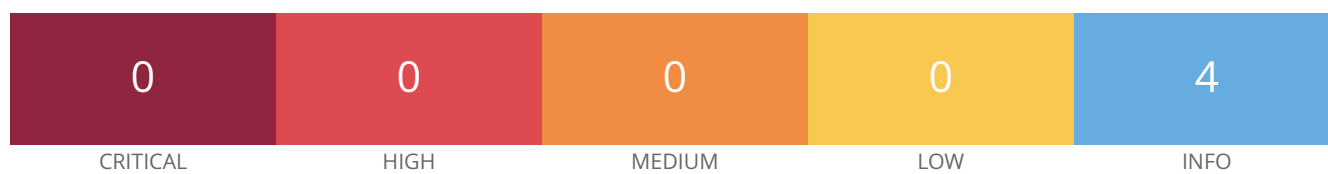
### Vulnerabilities

Total: 5

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information

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

## 10.0.0.40



### Vulnerabilities

Total: 4

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

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

## 10.0.0.41



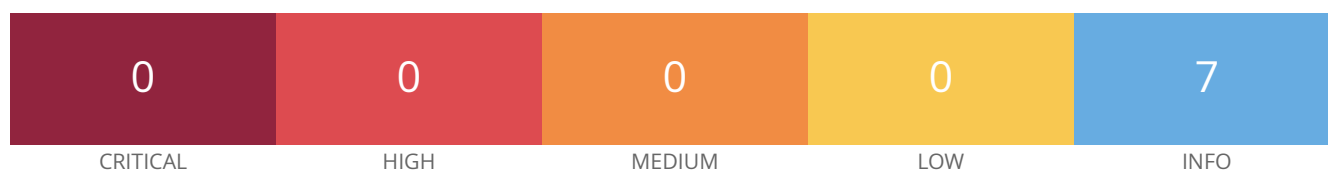
### Vulnerabilities

Total: 13

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	4.0	50686	IP Forwarding Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	50350	OS Identification Failed
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	10287	Traceroute Information

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

## 10.0.0.42



### Vulnerabilities

Total: 7

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	102821	OS Identification : OUI
INFO	N/A	-	10287	Traceroute Information

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

## 10.0.0.46



### Vulnerabilities

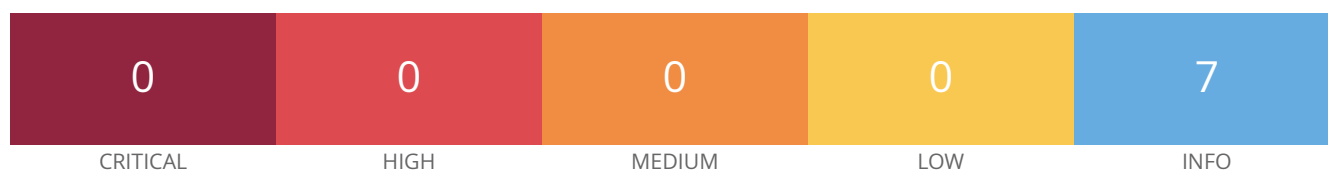
Total: 23

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	10287	Traceroute Information

INFO	N/A	-	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	-	35712	Web Server UPnP Detection
INFO	N/A	-	66717	mDNS Detection (Local Network)
INFO	N/A	-	106375	nginx HTTP Server Detection

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

## 10.0.0.47



### Vulnerabilities

Total: 7

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	102821	OS Identification : OUI
INFO	N/A	-	10287	Traceroute Information

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



## 10.0.0.51



### Vulnerabilities

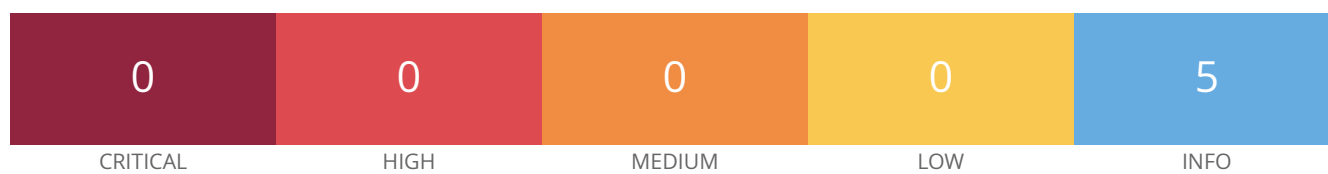
Total: 33

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.3	-	57608	SMB Signing not required
INFO	N/A	-	12634	Authenticated Check : OS Name and Installed Package Enumeration
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	54615	Device Type
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	19506	Nessus Scan Information

INFO	N/A	-	<a href="#">11936</a>	OS Identification
INFO	N/A	-	<a href="#">97993</a>	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	-	<a href="#">117886</a>	OS Security Patch Assessment Not Available
INFO	N/A	-	<a href="#">56984</a>	SSL / TLS Versions Supported
INFO	N/A	-	<a href="#">10863</a>	SSL Certificate Information
INFO	N/A	-	<a href="#">70544</a>	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	<a href="#">21643</a>	SSL Cipher Suites Supported
INFO	N/A	-	<a href="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	<a href="#">156899</a>	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	<a href="#">121010</a>	TLS Version 1.1 Protocol Detection
INFO	N/A	-	<a href="#">136318</a>	TLS Version 1.2 Protocol Detection
INFO	N/A	-	<a href="#">110723</a>	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	<a href="#">64814</a>	Terminal Services Use SSL/TLS
INFO	N/A	-	<a href="#">135860</a>	WMI Not Available
INFO	N/A	-	<a href="#">10150</a>	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	<a href="#">66717</a>	mDNS Detection (Local Network)

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

## 10.0.0.55



### Vulnerabilities

Total: 5

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information

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