



NEVER DO

DEEPAK

Domain: MEESHO.COM




Statement: Finding the IP Address and the domain details of the website meesho.com

Tool Used: whois.domaintools.com

Results:-

Registrant

Registration Private

Registrant Org	Domains By Proxy, LLC	
Registrant Country	us	
Registrar	GoDaddy.com, LLC IANA ID: 146 URL: https://www.godaddy.com,http://www.godaddy.com Whois Server: whois.godaddy.com abuse@godaddy.com (p) 14806242505	
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited	
Dates	2,484 days old Created on 2015-10-17 Expires on 2024-10-17 Updated on 2021-10-05	—
Name Servers	NS-1178.AWSDNS-19.ORG (has 48,778 domains) NS-157.AWSDNS-19.COM (has 1,658 domains) NS-1920.AWSDNS-48.CO.UK (has 285 domains) NS-662.AWSDNS-18.NET (has 37 domains)	
104	Registration Private Domains By Proxy, LLC DomainsByProxy.com, Tempe, Arizona, 85284, us (p) 14806242599 (f) 14806242598	
IP Address	104.18.26.119 - 9 other sites hosted on this server	—
IP Location	 - California - San Jose - Cloudflare Inc.	
ASN	 AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)	
Domain Status	Registered And Active Website	
IP History	63 changes on 63 unique IP addresses over 18 years	—
Registrar History	2 registrars with 3 drops	—
Hosting History	17 changes on 8 unique name servers over 16 years	—
Website	Website	
Website Title	 500 SSL negotiation failed:	—
Response Code	500	
Terms	158 (Unique: 93, Linked: 4)	

Images 0 (Alt tags missing: 0)

Links 2 (Internal: 0, Outbound: 2)

Findings:

Domain name: meesho.com

IP Address: 104.18.26.119

IP Location: California –San Jose – Cloudflare Inc

Domain Status: Registered and Active

Created on 17-10-2015

Expires on 17-10-2024

Statement: Find the Subdomains of meesho.com

Tool used: Virustotal

Here the Sub domains of meesho.com

onlinejobguru.meesho.com
nexstyle.meesho.com
sarvesaautomart.meesho.com
thehandloomsofmaheshwar.meesho.com
simrancollections.meesho.com
champcash4.meesho.com
mantraboutique.meesho.com
motoignite.meesho.com
siddhicreation.meesho.com
desiera.meesho.com
trendydesignerscollection.meesho.com
chosenbyyou.meesho.com
balbirsilkstorephagwara.meesho.com
ratanmaganlalmali.meesho.com
nirvanaschoolofthaiyogaclinicalmassage.meesho.com
ethniquestyle.meesho.com
travelsyrup.meesho.com
thirukumaransilks.meesho.com
anusboutique.meesho.com
www.champcash.meesho.com
kinjalwalldecore.meesho.com
fashionhub15.meesho.com
cliffpeacocksboutique.meesho.com
dihadesigners.meesho.com
trendyjewelsclothes.meesho.com
ezzycollection.meesho.com
markettwister.meesho.com
aarudracollections.meesho.com
choice4fab.meesho.com
shoprail.meesho.com
kaizenelectronics.meesho.com
spinnella.meesho.com
thestitchstory.meesho.com
champcash.meesho.com
www.gardensarees.meesho.com

Statement: Find out the email of meesho.com

Tool used: hunter.io

Results: help@meesho.com

Support@meesho.com

Statement: Check the http status of meesho.com

Tool used: http.io

Result:

<http://meesho.com>

status code: 301, 200

Statement: Online SSL Bulk check of meesho.com

Tool used: ssl checker

[www.meesho.com resolves to 104.18.26.119](#)

[Server Type: cloudflare](#)

[The certificate should be trusted by all major web browsers \(all the correct intermediate certificates are installed\).](#)

[The certificate will expire in 248 days.](#) [Remind me](#)

[The hostname \(www.meesho.com\) is correctly listed in the certificate.](#)

Findings: the site meesho.com is secured by SSL certification and the certificate will expire in 248 days from now (August 6, 2022)

Statement: Verify and check the Domain names and new Domain extensions and Social Media availabilities.

Tool Used: namecheck.com

Findings: No Domain names are available

New Domain extensions

Statement: Find is there any data breach through the email of meesho.com

Source: haveibeenpwned.com

Findings:- No data breach has found for help@meesho.com

Statement: Find the IOT devices for meesho.com

Source: Shodan search engine

Shodan is a search engine that lets users search for various types of servers (webcams, routers, servers, etc) connected to the internet using a variety of filters.

*No results found on shodan for meesho.com

Statement: DNS Analysis of meesho.com

Tool used: DNS Recon

Findings:

: - Name servers of meesho.com

There are 8 Name Servers for meesho.com

NS ns-1178.awsdns-19.org 205.251.196.154

[-] Recursion enabled on NS Server 205.251.196.154

[*] NS ns-1178.awsdns-19.org 2600:9000:5304:9a00::1

[*] NS ns-157.awsdns-19.com 205.251.192.157

[-] Recursion enabled on NS Server 205.251.192.157

[*] NS ns-157.awsdns-19.com 2600:9000:5300:9d00::1

[*] NS ns-1920.awsdns-48.co.uk 205.251.199.128

[-] Recursion enabled on NS Server 205.251.199.128

[*] NS ns-1920.awsdns-48.co.uk 2600:9000:5307:8000::1

[*] NS ns-662.awsdns-18.net 205.251.194.150

[-] Recursion enabled on NS Server 205.251.194.150

[*] NS ns-662.awsdns-18.net 2600:9000:5302:9600::1

: - Mail Exchange Servers of meesho.com

MX aspmx.l.google.com 74.125.68.26

[*] MX aspmx2.googlemail.com 173.194.202.26

[*] MX aspmx3.googlemail.com 142.250.141.27

[*] MX alt1.aspmx.l.google.com 173.194.202.27

```

[*] MX alt2.aspmx.l.google.com 142.250.141.27
[*] MX aspmx.l.google.com 2404:6800:4003:c0f::1a
[*] MX aspmx2.googlemail.com 2607:f8b0:400e:c00::1b
[*] MX aspmx3.googlemail.com 2607:f8b0:4023:c0b::1a
[*] MX alt1.aspmx.l.google.com 2607:f8b0:400e:c00::1a
[*] MX alt2.aspmx.l.google.com 2607:f8b0:4023:c0b::1b

```

Tool: NMAP

Nmap stands for network Mapping, uses of this is to scan the entire the Network and helps in finding the operating services by the hosts.

- **Open ports**
- **Services**
- **Versions**
- **Operating System**
- **TCP/ UDP communications**
- **Nmap Scripts are used to examine the vulnerabilities of the target**

1:- Open ports and services of the meesho.com

PORT	STATE	SERVICE
25/tcp	open	smtp?
53/tcp	open	domain
80/tcp	open	http
110/tcp	open	pop3?
119/tcp	open	nnntp?
143/tcp	open	imap?
443/tcp	open	ssl/http
465/tcp	open	smtps?
563/tcp	open	snews?
587/tcp	open	submission?
993/tcp	open	imaps?
995/tcp	open	pop3s?

Only the above ports are open out of 655

2: Version detection

Command : `nmap -sV meesho.com`

The Versions of meesho.com

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	(generic dns response: NOTIMP)
80/tcp	open	http	Node.js Express framework
443/tcp	open	ssl/http	Node.js Express framework

```
(kali@kali)-[~]
$ nmap -sV meesho.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-05 15:19 EDT
Nmap scan report for meesho.com (3.1.251.136)
Host is up (0.065s latency).
Other addresses for meesho.com (not scanned): 18.140.86.237 3.1.105.223 18.136.39.11 52.77.30.131 13.215.105.243
rDNS record for 3.1.251.136: ec2-3-1-251-136.ap-southeast-1.compute.amazonaws.com
Not shown: 987 filtered tcp ports (no-response), 1 filtered tcp ports (host-unreach)
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp?
53/tcp    open  domain       (generic dns response: NOTIMP)
80/tcp    open  http         Node.js Express framework
110/tcp   open  pop3?
119/tcp   open  nntp?
143/tcp   open  imap?
443/tcp   open  ssl/http     Node.js Express framework
465/tcp   open  smtps?
563/tcp   open  snews?
587/tcp   open  submission?
993/tcp   open  imaps?
995/tcp   open  pop3s?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.92%I=7%D=8/5%Time=62ED6D9C%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,E,"\0\0c\0\0\06\0\0\081\0\0\0\0\0\0\0\0\0\0");
```

3. Operating System of meesho.com

Command : `nmap -O meesho.com`

Findings:- Operating system –Oracle virtual box

```
Running: Oracle Virtualbox
OS CPE: cpe:/o:oracle:virtualbox
OS details: Oracle Virtualbox
```


4. Finding the vulnerabilities of meesho.com with nmap

Command: - nmap -sV --script-vulnscan/vulnscan.nse meesho.com

TOOL: METASPLOIT

Metasploit tool is used to find the vulnerability and to exploit the vulnerability.

Statement: Run the Auxiliary to meesho.com

To run the auxiliary follow the below steps

Matching auxiliary modules of SMTP port.

Name	Rank	Description
1. auxiliary/server/capture/smtp	Normal	Authentication Capture :SMTP
2. auxiliary/client/smtp/emailer	normal	generic emailer(SMTP)
3. auxiliary/scanner/smtp/smtp_enum	normal	SMTP user enumeration utility
4. auxiliary/scanner/smtp/smtp_relay	normal	open relay detection
5. auxiliary/scanner/smtp/smtp_version	normal	SMTP Banner Grabber
6. auxiliary/scanner/smtp/smtp_ntlm_domain	normal	NTLM domain

21	auxiliary/scanner/smtp/smtp_version	normal	No	SMTP Banner Grabber
22	auxiliary/scanner/smtp/smtp_ntlm_domain	normal	No	SMTP NTLM Domain Enumeration
23	auxiliary/scanner/smtp/smtp_relay	normal	No	SMTP Open Relay Detection
24	auxiliary/fuzzers/smtp/smtp_fuzzer	normal	No	SMTP Simple Fuzzer
25	auxiliary/scanner/smtp/smtp_enum	normal	No	SMTP User Enumeration Utility
26	auxiliary/doc/smtp/sendmail_process	normal	No	Sendmail SMTP Address

```

msf6 > use 1
msf6 auxiliary(server/capture/smtp) > show options

Module options (auxiliary/server/capture/smtp):

  Name      Current Setting  Required  Description
  --      -
  AUTHPROMPT false           yes       Require authentication from clients
  SRVHOST    0.0.0.0         yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT    25              yes       The local port to listen on.
  SSL        false           no        Negotiate SSL for incoming connections
  SSLCert    no              no        Path to a custom SSL certificate (default is randomly generated)

Auxiliary action:

  Name      Description
  --      -
  Capture   Run SMTP capture server

msf6 auxiliary(server/capture/smtp) > run
[*] Auxiliary module running as background job 0.

[*] Started service listener on 0.0.0.0:25
[*] Server started.
msf6 auxiliary(server/capture/smtp) >

```

Result after execute the auxiliary

Server is started listening on 0.0.0.25

TOOL: MALTEGO

Maltego is an open-source intelligence forensic application. Which will help you to get more accurate information and in a smarter way. In simple words, it is an information-gathering tool. Features of Maltego: It is used for gathering information for security related work.

Statement: Information gathering through Maltego tool for the domain meesho.com

Findings:- DNS – meesho.com onlinebussiness.meesho.com

Tech.meesho.com trainming.meesho.com

ftp.meesho.com

hostmaster.meesho.com

notification.meesho.com

addeckko.meesho.com

Websites- www.meesho.com

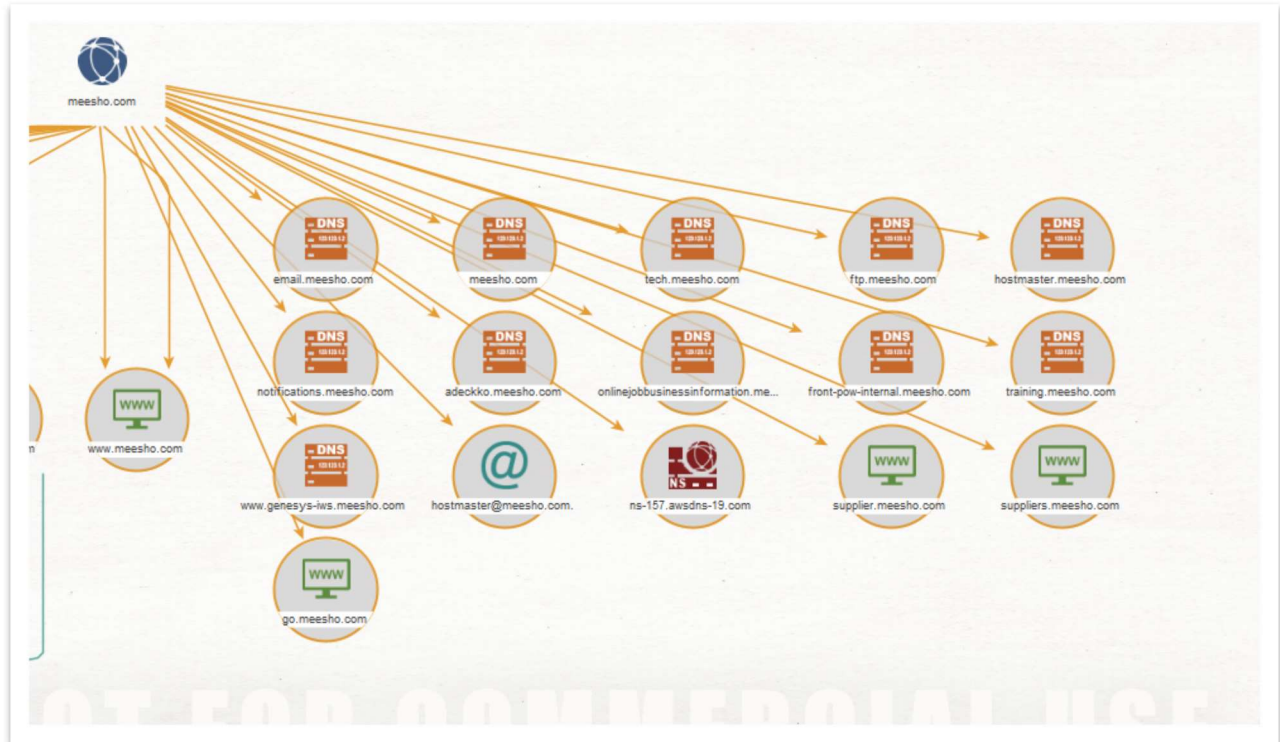
Suppliers.meesho.ocm

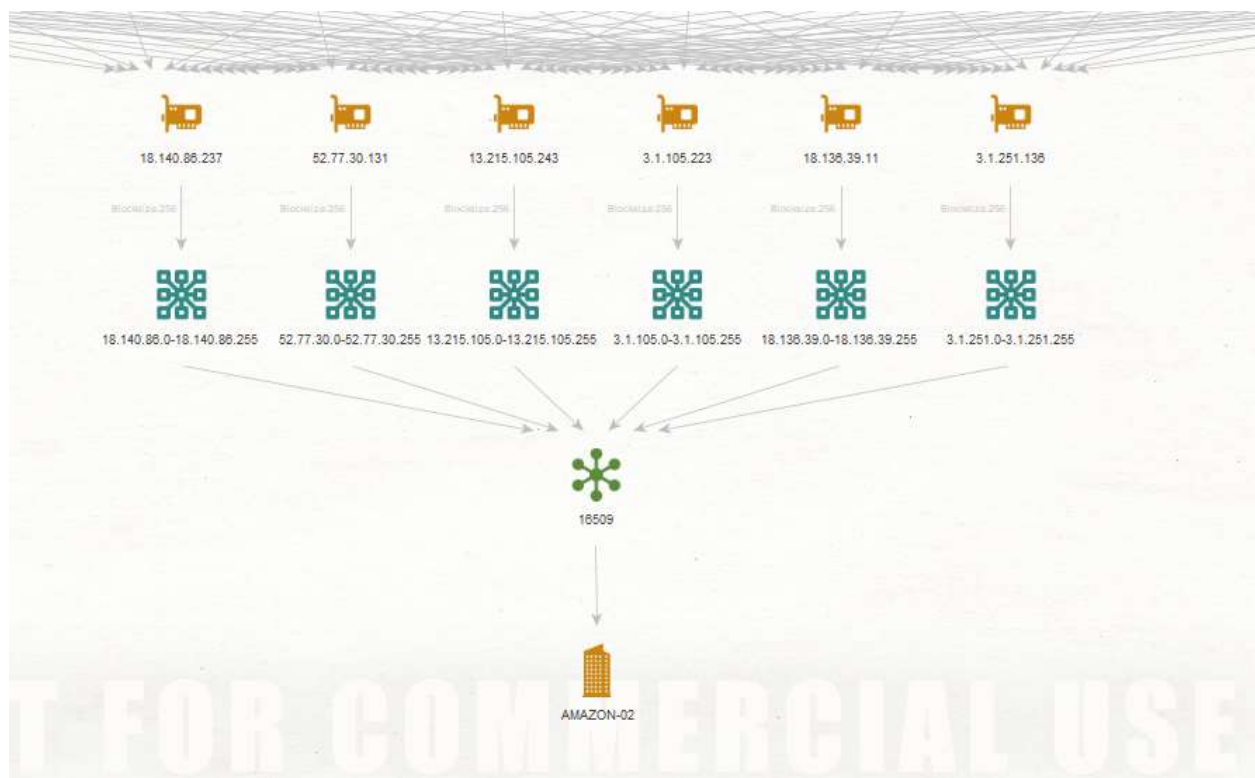
Supplier.meesho.com

go.meesho.com

NS – ns-157.awsdns-19.com

Screenshot:-





Running transform To DNS Name [Find common DNS names] on 1 entities (from entity "meesho.com")

Running transform To Website [Quick lookup] on 1 entities (from entity "meesho.com")

Running transform To Website using domain [Bing] on 1 entities (from entity "meesho.com")

Running transform To DNS Name - SOA (Start of Authority) on 1 entities (from entity "meesho.com")

Running transform To DNS Name [SecurityTrails] on 1 entities (from entity "meesho.com")

Domain resolves wildcards. Comparing against wildcard IP (from entity "meesho.com")

Transform to DNS Name [Find common DNS names] returned with 12 entities (from entity "meesho.com")

Transform to DNS Name - SOA (Start of Authority) returned with 2 entities (from entity "meesho.com")

Transform to DNS Name [Find common DNS names] done (from entity "meesho.com")

Transform to DNS Name - SOA (Start of Authority) done (from entity "meesho.com")

Running transform To DNS Name (interesting) [SecurityTrails] on 1 entities (from entity "meesho.com")

Running transform To DNS Name [Attempt zone transfer] on 1 entities (from entity "meesho.com")

Transform to Website [Quick lookup] returned with 1 entities (from entity "meesho.com")

Transform to Website [Quick lookup] done (from entity "meesho.com")

Included Bing Search Transforms: 99 of 100 credits remaining. Current quota period ends at 2022-08-28T03:34:18.526Z [UTC] (from entity "meesho.com")

Transform to Website using domain [Bing] returned with 4 entities (from entity "meesho.com")

Transform to Website using domain [Bing] done (from entity "meesho.com")

Transform to DNS Name [Attempt zone transfer] returned with 0 entities (from entity "meesho.com")

Transform to DNS Name [Attempt zone transfer] done (from entity "meesho.com")

Included MST SecurityTrails Transform runs: 98 of 100 credits remaining. Current quota period ends at 2022-08-28T03:34:18.526Z [UTC] (from entity "meesho.com")

Transform to DNS Name (interesting) [SecurityTrails] returned with 3 entities (from entity "meesho.com")

Transform to DNS Name (interesting) [SecurityTrails] done (from entity "meesho.com")

Included MST SecurityTrails Transform runs: 99 of 100 credits remaining. Current quota period ends at 2022-08-28T03:34:18.526Z [UTC] (from entity "meesho.com")

Transform to DNS Name [SecurityTrails] returned with 12 entities (from entity "meesho.com")

Transform to DNS Name [SecurityTrails] done (from entity "meesho.com")

Running transform To IP Address [DNS] on 12 entities (from 12 entities)

Transform to IP Address [DNS] returned with 6 entities (from 12 entities)

Transform to IP Address [DNS] returned with 6 entities (from 12 entities)

Transform to IP Address [DNS] returned with 6 entities (from 12 entities)

Transform to IP Address [DNS] returned with 6 entities (from 12 entities)

Transform to IP Address [DNS] returned with 6 entities (from 12 entities)

Transform to IP Address [DNS] returned with 6 entities (from 12 entities)

Transform to IP Address [DNS] returned with 6 entities (from 12 entities)

Transform to IP Address [DNS] returned with 6 entities (from 12 entities)

Transform to IP Address [DNS] returned with 6 entities (from 12 entities)

Transform to IP Address [DNS] returned with 6 entities (from 12 entities)

Transform to IP Address [DNS] returned with 6 entities (from 12 entities)

Transform to IP Address [DNS] returned with 6 entities (from 12 entities)

Transform to IP Address [DNS] done (from 12 entities)

Running transform To Netblock [Using natural boundaries] on 6 entities (from 6 entities)

Transform to Netblock [Using natural boundaries] returned with 1 entities (from 6 entities)

Transform to Netblock [Using natural boundaries] returned with 1 entities (from 6 entities)

Transform to Netblock [Using natural boundaries] returned with 1 entities (from 6 entities)

Transform to Netblock [Using natural boundaries] returned with 1 entities (from 6 entities)

Transform to Netblock [Using natural boundaries] returned with 1 entities (from 6 entities)

Transform to Netblock [Using natural boundaries] returned with 1 entities (from 6 entities)

Transform to Netblock [Using natural boundaries] done (from 6 entities)

Running transform To AS Number [WhoisXML] on 6 entities (from 6 entities)

Included MST WhoisXML IP Netblocks Transform runs: 495 of 500 credits remaining. Current quota period ends at 2022-08-28T03:34:18.526Z[UTC] (from entity "3.1.251.0-3.1.251.255")

Transform to AS Number [WhoisXML] returned with 1 entities (from 6 entities)

Included MST WhoisXML IP Netblocks Transform runs: 496 of 500 credits remaining. Current quota period ends at 2022-08-28T03:34:18.526Z[UTC] (from entity "13.215.105.0-13.215.105.255")

Transform to AS Number [WhoisXML] returned with 1 entities (from 6 entities)

Included MST WhoisXML IP Netblocks Transform runs: 498 of 500 credits remaining. Current quota period ends at 2022-08-28T03:34:18.526Z[UTC] (from entity "18.140.86.0-18.140.86.255")

Transform to AS Number [WhoisXML] returned with 1 entities (from 6 entities)

Included MST WhoisXML IP Netblocks Transform runs: 497 of 500 credits remaining. Current quota period ends at 2022-08-28T03:34:18.526Z[UTC] (from entity "3.1.105.0-3.1.105.255")

Transform to AS Number [WhoisXML] returned with 1 entities (from 6 entities)

Included MST WhoisXML IP Netblocks Transform runs: 499 of 500 credits remaining. Current quota period ends at 2022-08-28T03:34:18.526Z [UTC] (from entity "52.77.30.0-52.77.30.255")

Transform to AS Number [WhoisXML] returned with 1 entities (from 6 entities)

Included MST WhoisXML IP Netblocks Transform runs: 494 of 500 credits remaining. Current quota period ends at 2022-08-28T03:34:18.526Z [UTC] (from entity "18.136.39.0-18.136.39.255")

Transform to AS Number [WhoisXML] returned with 1 entities (from 6 entities)

Transform to AS Number [WhoisXML] done (from 6 entities)

Running transform To Company (Owner) [WhoisXML] on 1 entities (from entity "16509")

Included MST WhoisXML IP Netblocks Transform runs: 493 of 500 credits remaining. Current quota period ends at 2022-08-28T03:34:18.526Z [UTC] (from entity "16509")

Transform To Company (Owner) [WhoisXML] returned with 1 entities (from entity "16509")

Transform To Company (Owner) [WhoisXML] done (from entity "16509")

pharmeasy

[Back to My Scans](#)

Configure

Audit Trail

Launch

Report

Export

Hosts1

Vulnerabilities11

VPR Top Threats

History1

Filter

Search Vulnerabilities

11 Vulnerabilities

Sev	Score	Name	Family	Count		
INFO	...	HTTP (Multiple Issues)	Web Servers	2		
INFO		Nessus SYN scanner	Port scanners	5		
INFO		Device Type	General	1		
INFO		Host Fully Qualified Domain Name (FQDN) Resolution	General	1		
INFO		ICMP Timestamp Request Remote Date Disclosure	General	1		
INFO		Nessus Scan Information	Settings	1		
INFO		OS Identification	General	1		
INFO		Reverse NAT/Intercepting Proxy Detection	Firewalls	1		
INFO		Service Detection	Service detection	1		
INFO		TCP/IP Timestamps Supported	General	1		
INFO		Traceroute Information	General	1		

Scan Details

Policy:Advanced Scan

Status:Completed

Severity Base:CVSS v3.0

Scanner:Local Scanner

Start:Today at 11:39 AM

End:Today at 11:54 AM

Elapsed:14 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Activate Windows

Go to Settings to activate Windows.