

Cybersecurity Recon Report

Target: nbkrist.co.in

Generated: 2025-09-13 20:52:07

[+] Recon started: 2025-09-13 20:52:07

[+] Target: nbkrist.co.in

[+] IP Address: 208.109.31.44

[+] nslookup output:

DNS request timed out.
timeout was 2 seconds.
Server: UnKnown
Address: fe80::1

DNS request timed out.
timeout was 2 seconds.
Name: nbkrist.co.in
Address: 208.109.31.44

[+] WHOIS Information:

```
{
  "domain_name": "nbkrist.co.in",
  "registrar": "GoDaddy.com, LLC",
  "registrar_url": [
    "www.godaddy.com",
    "https://www.godaddy.com"
  ],
  "registrar_iana": "146",
  "updated_date": [
    "2025-05-30 09:24:49.853000",
    "2025-01-21 07:04:52"
  ],
  "creation_date": [
    "2021-01-29 07:04:39.146000",
    "2021-01-29 07:04:39"
  ],
  "expiration_date": [
    "2026-01-29 07:04:39.146000",
    "2026-01-29 07:04:39"
  ],
  "name_servers": [
    "ns34.domaincontrol.com",
    "ns33.domaincontrol.com"
  ],
  "organization": null,
  "state": "Andhra Pradesh",
  "status": [
    "clientRenewProhibited https://icann.org/epp#clientRenewProhibited",
    "clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited",
    "clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited",
```

```
"clientTransferProhibited https://icann.org/epp#clientTransferProhibited"
],
"emails": [
  "reg_admin@godaddy.com",
  "abuse@godaddy.com"
],
"country": "IN",
"dnssec": "unsigned"
}
```

[+] SSL Certificate:

```
{'subject': (((('commonName', 'nbkrist.co.in'),)),), 'issuer': (((('countryName', 'US'),),
((('stateOrProvinceName', 'Arizona'),), ((('localityName', 'Scottsdale'),), ((('organizationName',
'GoDaddy.com, Inc.'),), ((('organizationalUnitName', 'http://certs.godaddy.com/repository/'),),
((('commonName', 'Go Daddy Secure Certificate Authority - G2'),)), 'version': 3, 'serialNumber':
'BFF7693EFF5347F3', 'notBefore': 'Aug 13 10:12:50 2025 GMT', 'notAfter': 'Aug 12 10:07:43 2026
GMT', 'subjectAltName': (('DNS', 'nbkrist.co.in'), ('DNS', 'www.nbkrist.co.in')), 'OCSP':
('http://ocsp.godaddy.com/',), 'caIssuers': ('http://certificates.godaddy.com/repository/gdig2.crt',),
'crlDistributionPoints': ('http://crl.godaddy.com/gdig2s1-58418.crl',),}}
```

[+] Open Ports:

[21, 22, 80, 443, 3306]

[+] HTTP Headers:

```
{'Date': 'Sat, 13 Sep 2025 15:22:28 GMT', 'Server': 'Apache', 'X-Powered-By': 'PHP/8.0.30',
'Upgrade': 'h2,h2c', 'Connection': 'Upgrade, Keep-Alive', 'Vary': 'Accept-Encoding',
'Content-Encoding': 'gzip', 'Content-Length': '27048', 'Keep-Alive': 'timeout=5', 'Content-Type':
'text/html; charset=UTF-8'}
```

[+] Technology fingerprints:

Header hints: {'Server': 'Apache', 'X-Powered-By': 'PHP/8.0.30'}

Guesses: Apache, PHP, Server header: Apache, X-Powered-By: PHP/8.0.30

[+] Banner grab:

Port 80: HTTP/1.1 301 Moved Permanently
Date: Sat, 13 Sep 2025 15:22:33 GMT
Server: Apache
Location: https://nbkrist.co.in/
Connection: close
Content-Type: text/html; charset=iso-8859-1

Port 443: HTTP/1.1 200 OK
Date: Sat, 13 Sep 2025 15:22:34 GMT
Server: Apache
X-Powered-By: PHP/8.0.30
Upgrade: h2,h2c
Connection: Upgrade, close
Vary: Accept-Encoding

Content-Type: text/html; charset=UTF-8

Port 22: SSH-2.0-OpenSSH_8.0

Port 21: 220----- Welcome to Pure-FTPd [privsep] [TLS] -----

220-You are user number 1 of 50 allowed.

220-Local time is now 08:22. Server port: 21.

220-This is a private system - No anonymous login

220-IPv6 connections are also welcome on this server.

220 You will be disconnected after 15 minutes of inactivity.

[+] Website Screenshot:

D:\Recon\dist\reports\nbkrist.co.in_screenshot.png

[✓] Recon Completed!