Scan Result

Test result for NMAP scans

nmap

vulnerabilities

```
PORT     STATE  SERVICE   VERSION
80/tcp   open   http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-server-header:
|   Microsoft-HTTPAPI/2.0
|_  Microsoft-IIS/10.0
113/tcp  closed ident
443/tcp  open   ssl/https
| http-server-header:
|   Apache
|_  Microsoft-HTTPAPI/2.0
8010/tcp open   ssl/xmpp?
| fingerprint-strings:
|   GenericLines, GetRequest:
|     HTTP/1.1 200 OK
|     Content-Length: 4492
|     Connection: close
|     Cache-Control: no-cache
|     Content-Type: text/html; charset=utf-8
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors 'self'
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="UTF-8">
|     <meta http-equiv="X-UA-Compatible" content="IE=8; IE=EDGE">
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <style type="text/css">
|     body {
|     height: 100%;
|     font-family: Helvetica, Arial, sans-serif;
|     color: #6a6a6a;
|     margin: 0;
|     display: flex;
|     align-items: center;
|     justify-content: center;
|_    input[type=date], input[type=email], input[type=number], input[type=password]
```

slowris

```
PORT     STATE  SERVICE
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
8010/tcp open   xmpp
```

Headers

```
Effective URL:  [94mhttps://niituniversity.in [0m
Missing security header: X-Permitted-Cross-Domain-Policies
Missing security header:  [93mExpect-CT [0m
Missing security header:  [93mCross-Origin-Embedder-Policy [0m
Missing security header:  [93mCross-Origin-Resource-Policy [0m
Missing security header:  [93mCross-Origin-Opener-Policy [0m
```

Testssl

```
Testing vulnerabilities

  Heartbleed  (CVE-2014-0160)                not vulnerable (OK) , no heartbeat extension
  CCS  (CVE-2014-0224)                       not vulnerable (OK)
  Ticketbleed  (CVE-2016-9244), experiment.  not vulnerable (OK) , no session ticket extension
  ROBOT                                      not vulnerable (OK)
  Secure Renegotiation (RFC 5746)            OpenSSL handshake didn't succeed
  Secure Client-Initiated Renegotiation      not vulnerable (OK)
  CRIME, TLS  (CVE-2012-4929)                not vulnerable (OK)
  BREACH  (CVE-2013-3587)                    potentially NOT ok, "gzip" HTTP compression detected.  - only supplied "/" tested
                                          Can be ignored for static pages or if no secrets in the page
  POODLE, SSL  (CVE-2014-3566)               not vulnerable (OK) , no SSLv3 support
  TLS_FALLBACK_SCSV  (RFC 7507)              No fallback possible (OK) , no protocol below TLS 1.2 offered
  SWEET32  (CVE-2016-2183, CVE-2016-6329)    not vulnerable (OK)
  FREAK  (CVE-2015-0204)                      not vulnerable (OK)
  DROWN  (CVE-2016-0800, CVE-2016-0703)       not vulnerable on this host and port (OK)
                                           make sure you don't use this certificate elsewhere with SSLv2 enabled services

https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=8A806D7B4454DBB37E1AA411F771FFC0821832ECABAEBE1F9AC44AAA618D3BE4
  LOGJAM  (CVE-2015-4000), experimental       VULNERABLE (NOT ok):  common prime:  RFC2409/Oakley Group 2  ( 1024 bits ),
                                           but no DH EXPORT ciphers
  BEAST  (CVE-2011-3389)                      not vulnerable (OK) , no SSL3 or TLS1
  LUCKY13  (CVE-2013-0169), experimental     potentially  VULNERABLE , uses cipher block chaining (CBC) ciphers with TLS. Check patches
  RC4  (CVE-2013-2566, CVE-2015-2808)         no RC4 ciphers detected (OK)
```