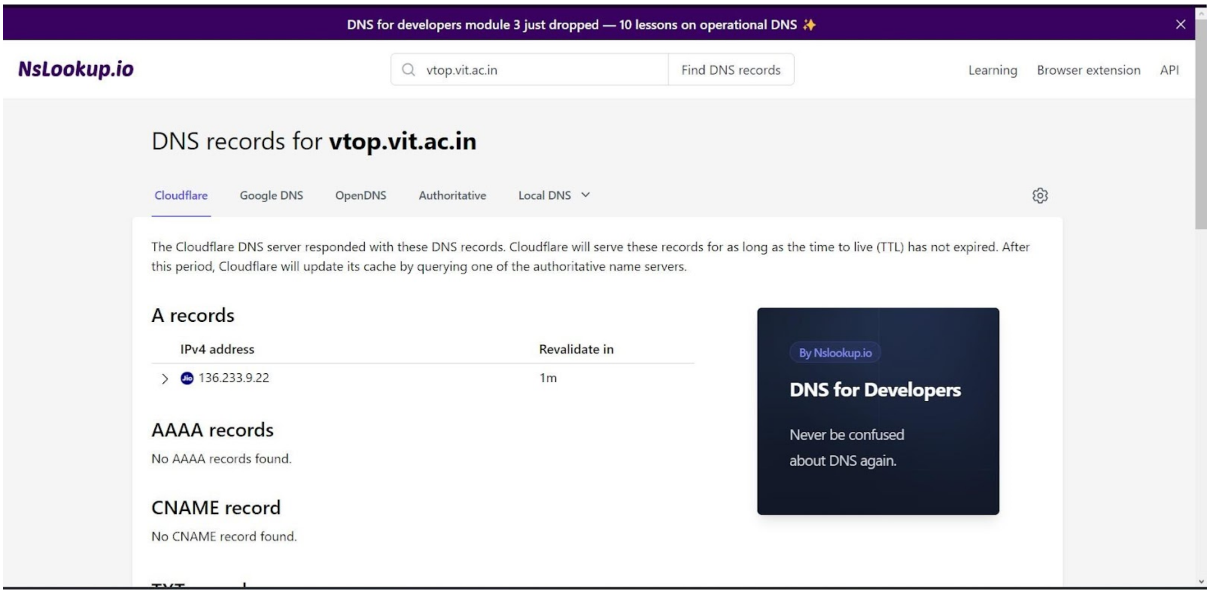
Saumyaa Prajapat
21BCI0265

# Task8:

## Scan any website to check the vulnerabilities in the website using nessus and make a report on it

Scan on the website of vit called vtop (https://vtop.vit.ac.in/vtop/login) we will first get the ipv4 address of the website we can do it using nslookup website 136.233.9.22



DNS records for **vtop.vit.ac.in**

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

A records

| IPv4 address | Revalidate in |
|---|---|
| 136.233.9.22 | 1m |

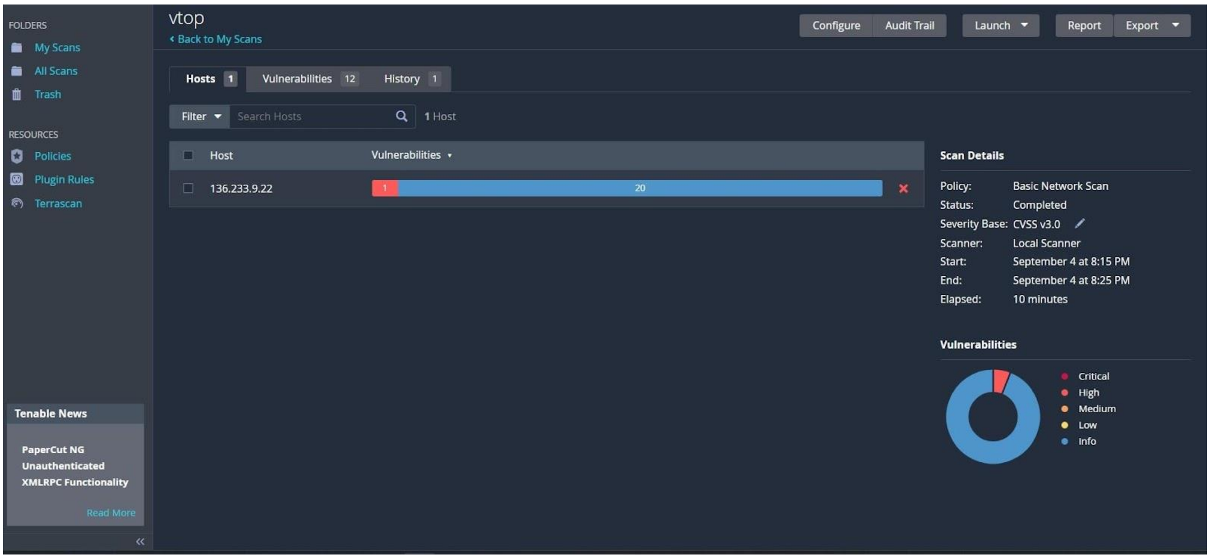
AAAA records

No AAAA records found.

CNAME record

No CNAME record found.

Now we will start the basic network scan on this website in nessus tool and it willl take some time to scan all the open ports of the website and to get the data of the vulnerabilities and this is how it will look after the scan



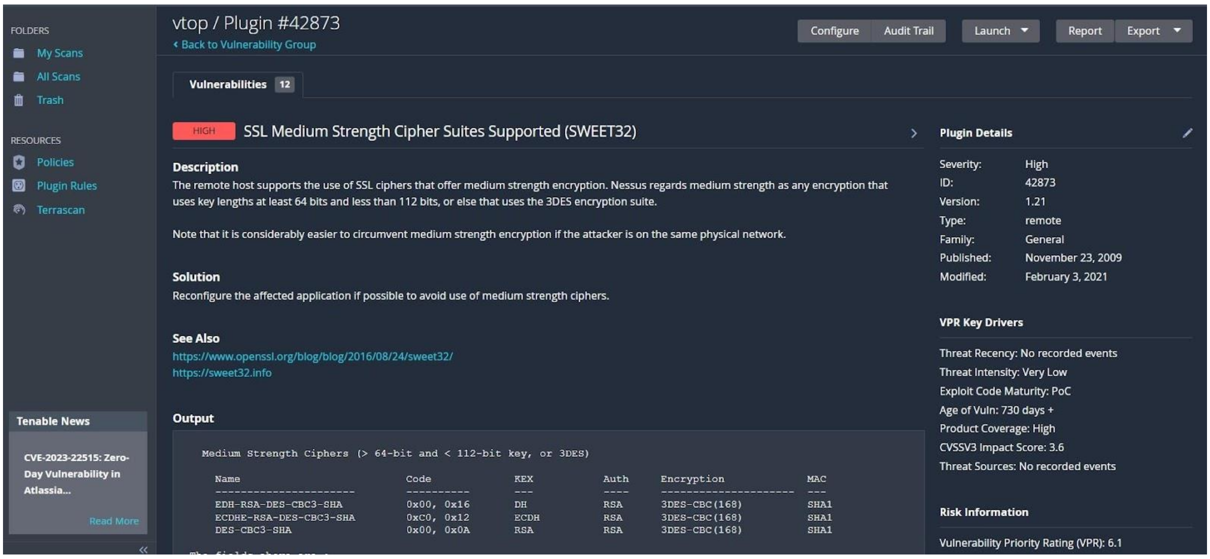
| Host | Vulnerabilities |
|---|---|
| 136.233.9.22 | 1 20 |

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: September 4 at 8:15 PM
End: September 4 at 8:25 PM
Elapsed: 10 minutes

Vulnerabilities

Saumyaa Prajapat
21BCI0265



SSL Medium Strength Cipher Suites Supported (SWEET32)

**Description**
The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

**Solution**
Reconfigure the affected application if possible to avoid use of medium strength ciphers.

**See Also**
https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

**Output**

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)          SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)          SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)          SHA1
```

**Plugin Details**

| | |
|---|---|
| Severity: | High |
| ID: | 42873 |
| Version: | 1.21 |
| Type: | remote |
| Family: | General |
| Published: | November 23, 2009 |
| Modified: | February 3, 2021 |

**VPR Key Drivers**

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: PoC
Age of Vuln: 730 days +
Product Coverage: High
CVSSV3 Impact Score: 3.6
Threat Sources: No recorded events

**Risk Information**

Vulnerability Priority Rating (VPR): 6.1

this is having a high vulnerability and its **SSL Medium Strength Cipher Suites Supported (SWEET32) with severity rating of 7.5**

vtop_ifvhbr.html

vtop_hma96n.nessus