A logo with a person in a hoodie using a computer

AI-generated content may be incorrect.

**MISSION HACKERS**

**BANGLADESH**

**Assignment No-05**

**Assignment Title: Scanning Ports & Protocols**

**Course Title: Cybersecurity & Ethical Hacking**

**Submitted by:**

**Name: Istiak Alam**

**Phone: 01765376101**

**Submission Date: 24-07-25**

**Lab Task Topic: Scanning IP and Find Vulnerabilities using Nmap / Zenmap.**

**Submitted to:**

**MD Sha Jalal**

**Founder of Mission Hackers Bangladesh**

## 🔍 **What is Nmap?**

**Nmap** (short for **Network Mapper**) is a **powerful open-source tool** used for:

* Scanning networks
* Discovering hosts and services
* Mapping network topology
* Finding open ports and vulnerabilities

🧑‍💻 It’s a hacker's microscope for network reconnaissance.

## 📦 **Why is Nmap Used in Ethical Hacking?**

| Purpose | Example |
| --- | --- |
| 🔎 Host Discovery | Find live systems in a network |
| 🔓 Port Scanning | Identify open ports (22, 80, 443, etc.) |
| 🎯 Service Detection | Identify what service is running on a port |
| 🛡️ OS Detection | Find the operating system of a host |
| 🚪 Vulnerability Scanning | Spot weak or outdated services |

## 💻 **Installing Nmap on Kali Linux**

Already installed by default in Kali Linux. To check:

**nmap --version**

If not installed:

**sudo apt update**

**sudo apt install nmap**

## 🧪 **Basic Nmap Commands (with Explanation)**

### ✅ 1. **Ping Scan (Host Discovery)**

**nmap -sn 192.168.1.0/24**

* Scans the whole subnet to find **which hosts are up**.
* -sn: Ping only, don’t scan ports.

### ✅ 2. **Basic** **Scan a Single Host**

**nmap 192.168.1.10**

* Default scan on a host: shows **open ports** and services.

### ✅ 3. **Scan Multiple Targets**

**nmap 192.168.1.10 192.168.1.20**

Or from a file:

**nmap -iL targets.txt**

### ✅ 4. **Port Scan (TCP by default)**

**nmap -p 80,443 192.168.1.10**

* Scan specific ports only.

**nmap -p- 192.168.1.10**

* Scan **all 65535** TCP ports.

### ✅ 5. **Service Version Detection**

**nmap -sV 192.168.1.10**

* Detects **version of services** running on open ports.

### ✅ 6. **Operating System Detection**

**nmap -O 192.168.1.10**

* Attempts to detect **OS type**.

### ✅ 7. **Aggressive Scan (All-in-One)**

**nmap -A 192.168.1.10**

* Performs:
  + OS Detection (-O)
  + Version Detection (-sV)
  + Script Scanning (-sC)
  + Trace-route

🛑 Warning: Very **loud** (detectable). Use carefully.

### ✅ 8. **Scan a Website**

**nmap scanme.nmap.org**

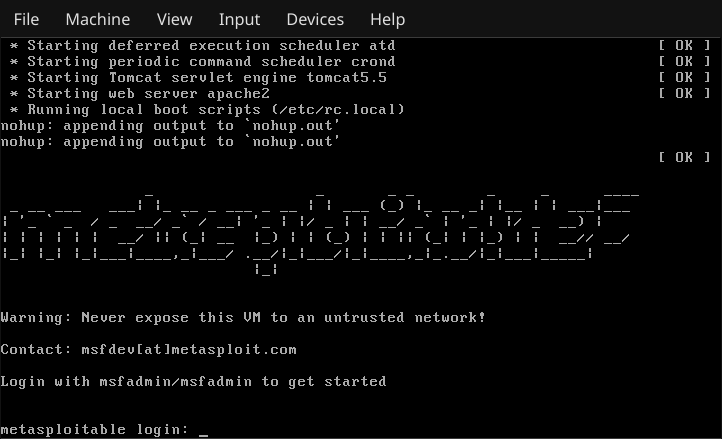
Note: scanme.nmap.org is an official **safe-to-scan** Nmap test server.

## 🧰 **Nmap Scan Types**

| Option | Scan Type | Description |
| --- | --- | --- |
| -sS | SYN Scan | Fast, stealthy (default) |
| -sT | TCP Connect | Full connection (less stealthy) |
| -sU | UDP Scan | Scans UDP ports |
| -sA | ACK Scan | Checks firewall rules |
| -sN | Null Scan | No flags set, stealth scan |

**Lets Find Vulnerabilities of Metasploitable 2 using Nmap :**

Step 1 : Open any Virtual Machine and boot Metasploitable2 Linux

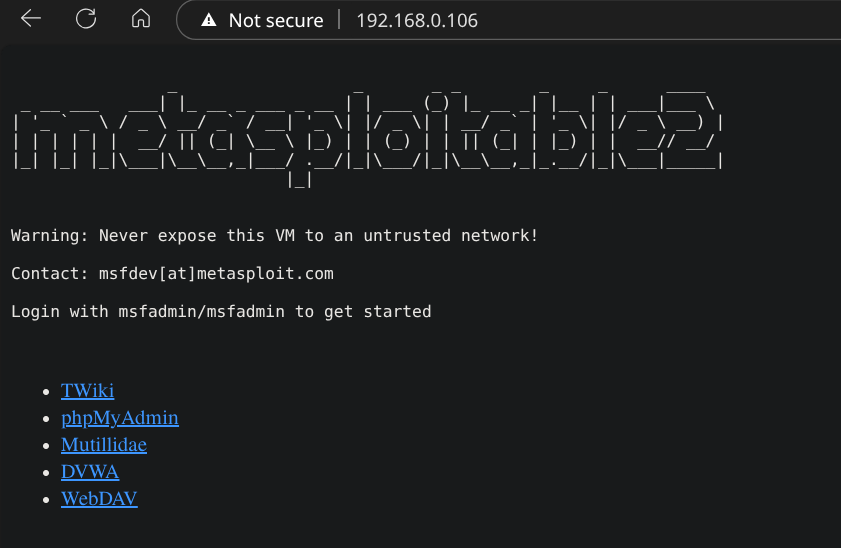


Step 2 : Login using **msfadmin** username and password

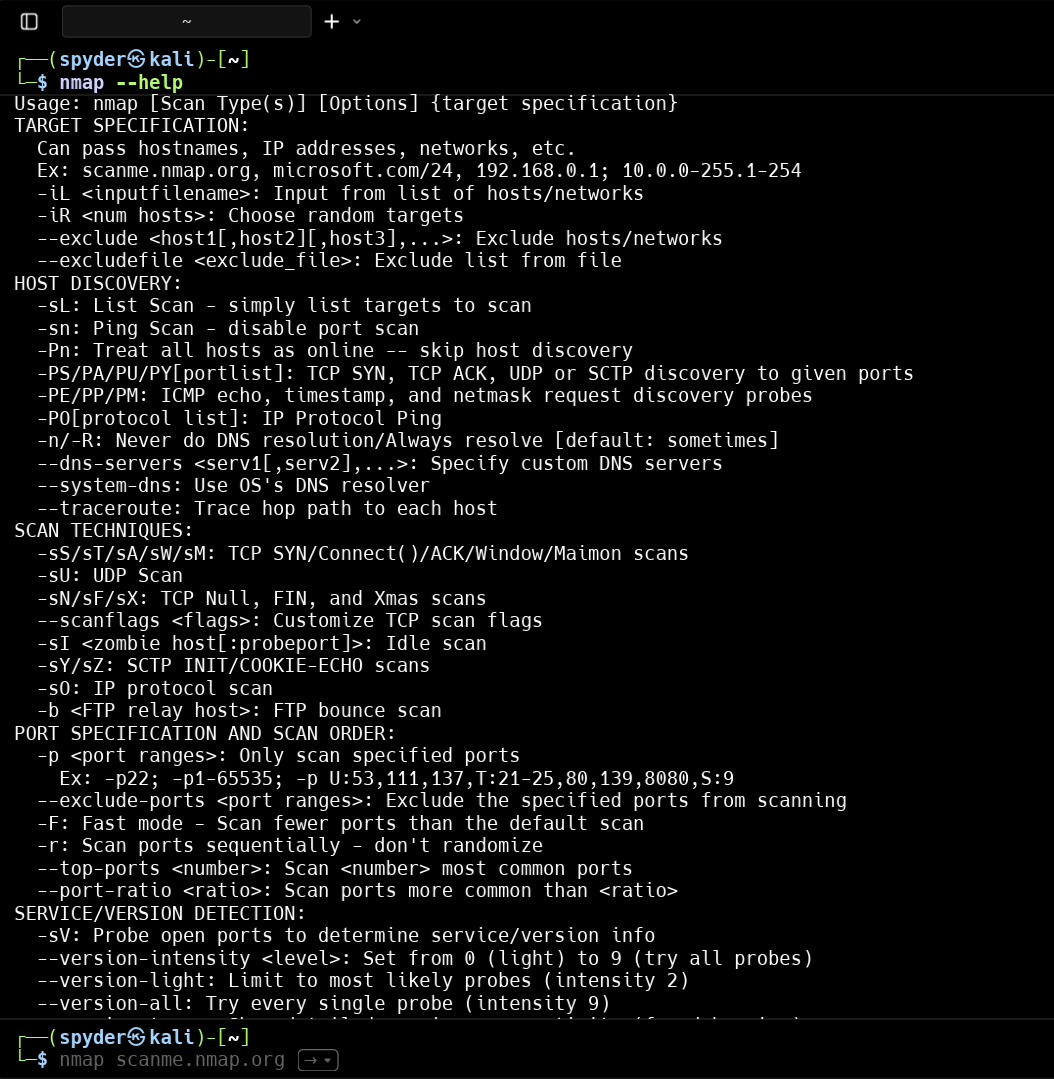
Step 3 : In the Metasploitable, find the IP address of the Vulnerable Machine by ‘ **ifconfig** ’

## **we will get the IP showing in eth0 inet addr : **192.168.0.106****

## **Step 4 : In the host machine open browser and go the this IP, this will show the metasploitable2 host page**

**There we can see some vulnerable machines..**

**Step 5 : Open Terminal by ctrl+alt+t and run nmap --help**

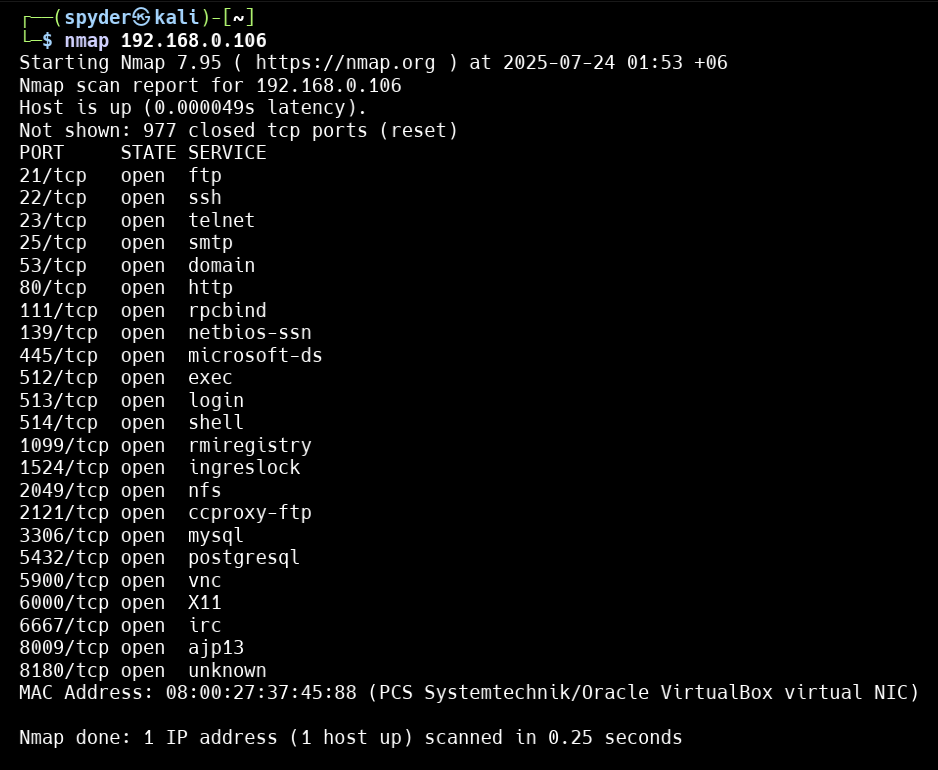


Here we can see all the recommended commands and syntax of using nmap..

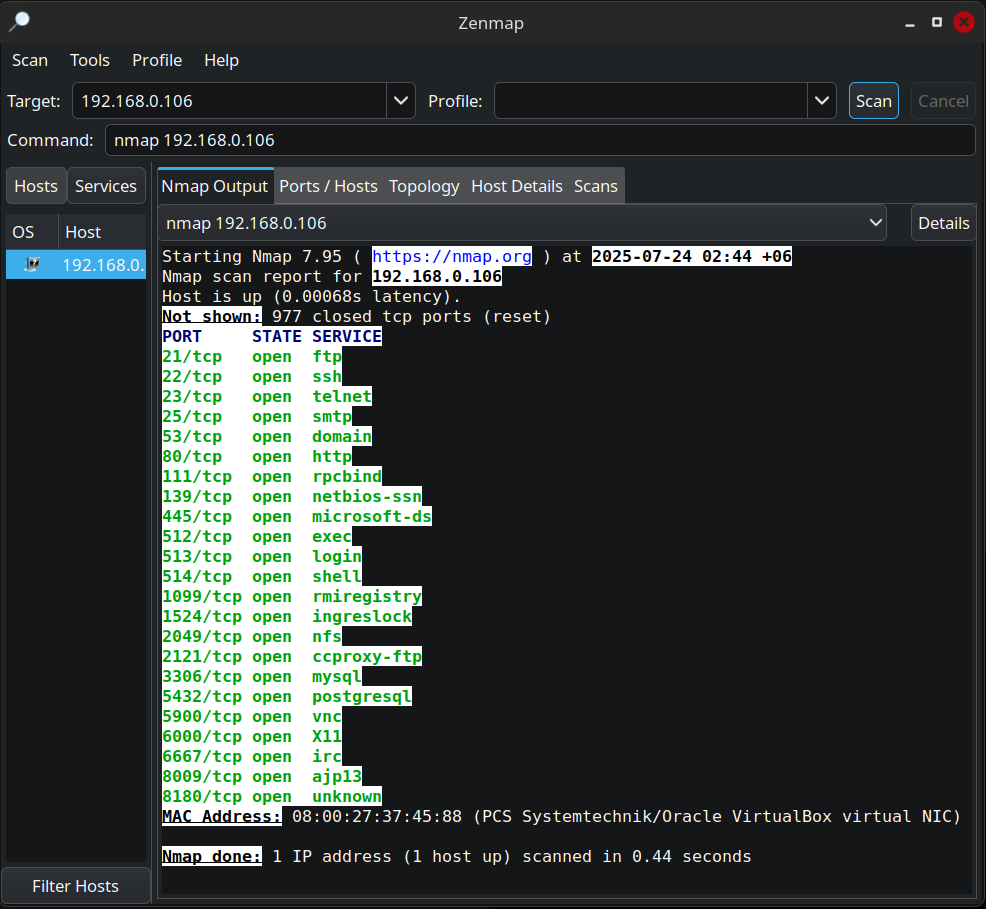
Using this Manual we can perform IP Address Vulnerabilities Scanning..

**Step 6 : Start the Basic Scan for the Metasploitable machine in Nmap**

**nmap 192.168.0.106**

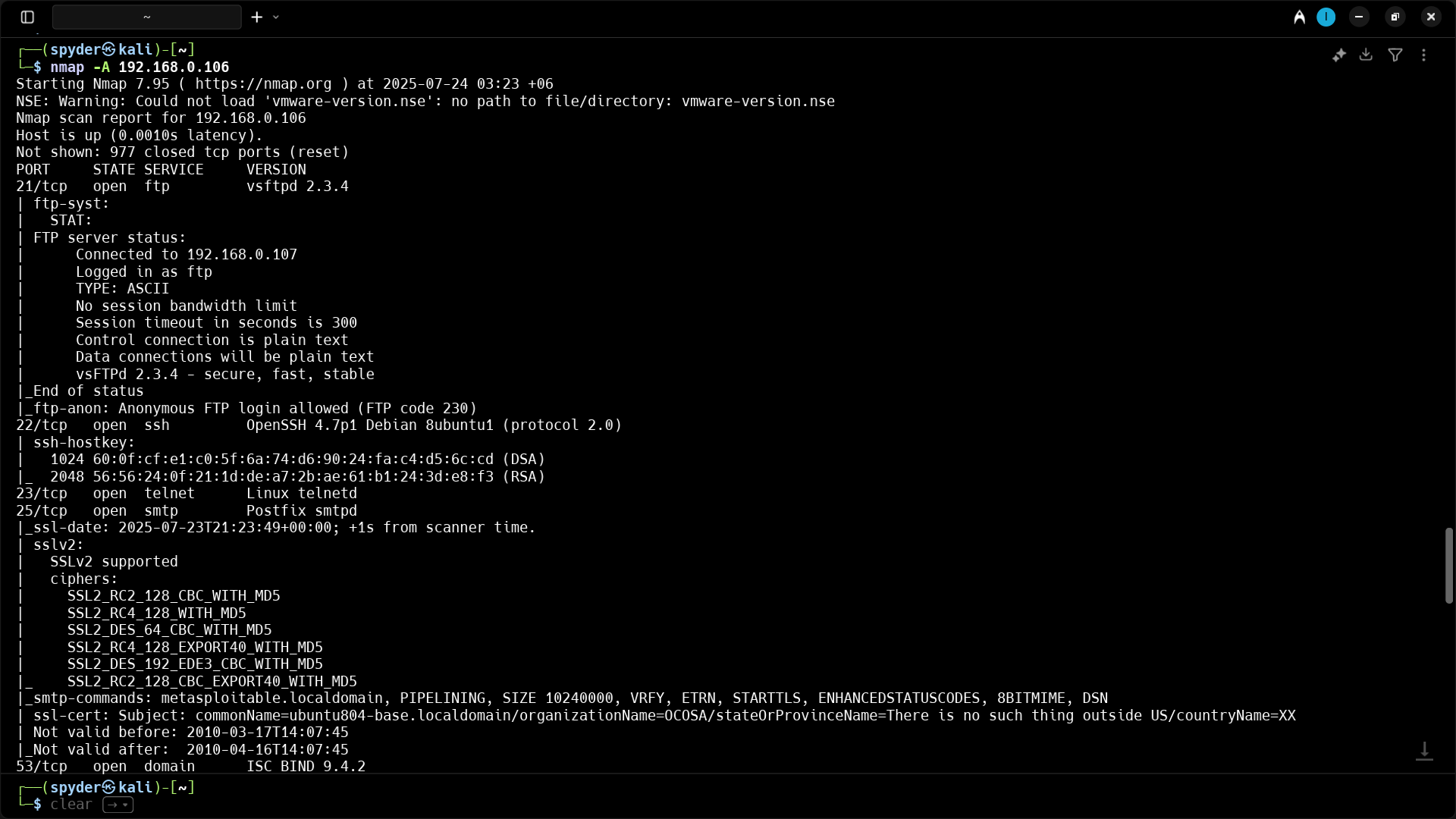


**In the other hand we can use Zenmap for a basic scan..**



**Step 7 : Lets Start Aggressive Scan (All-in-One) using**

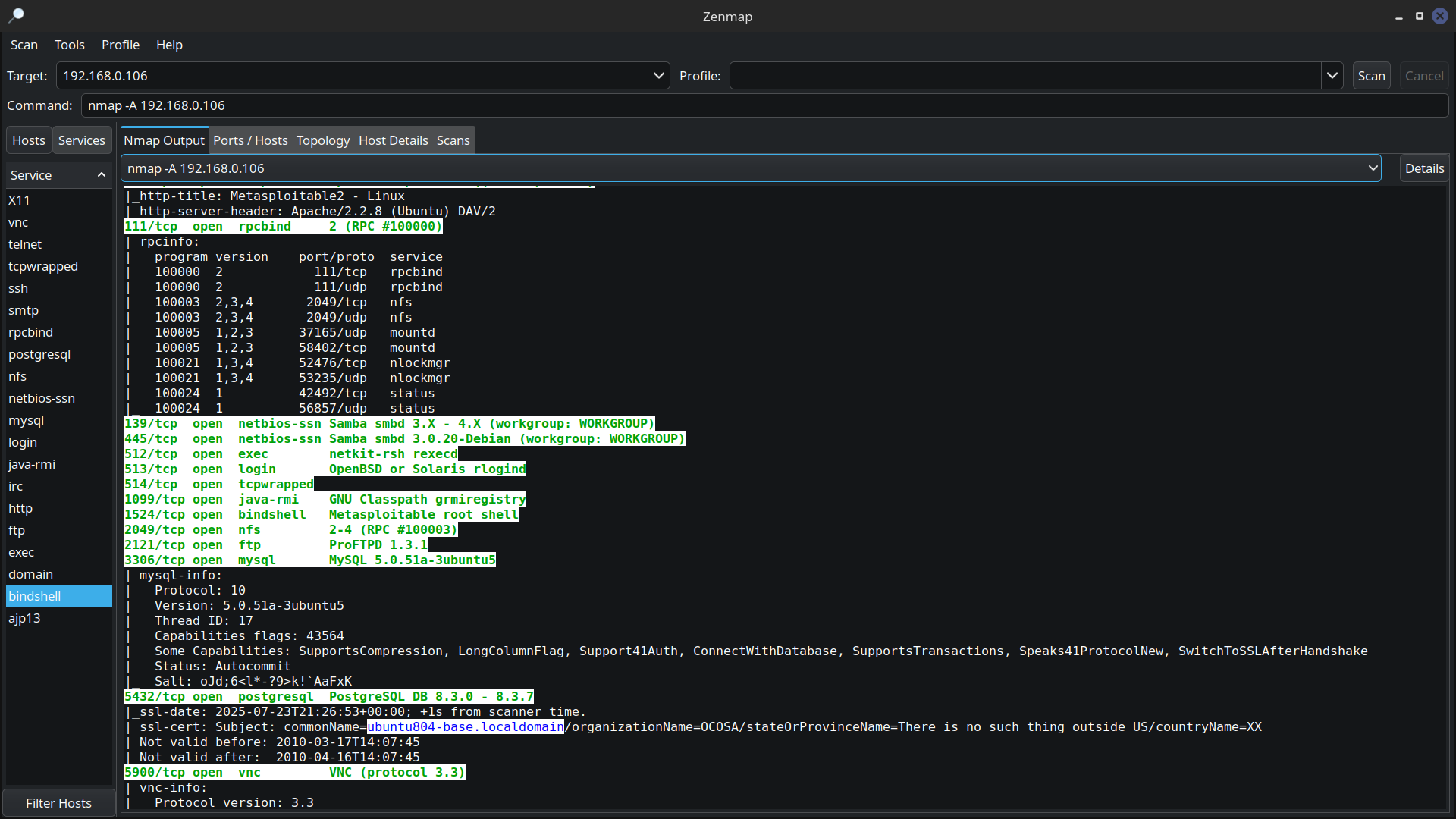
****nmap -A 192.168.0.106****



## **Start Aggressive Scan Using Zenmap :**

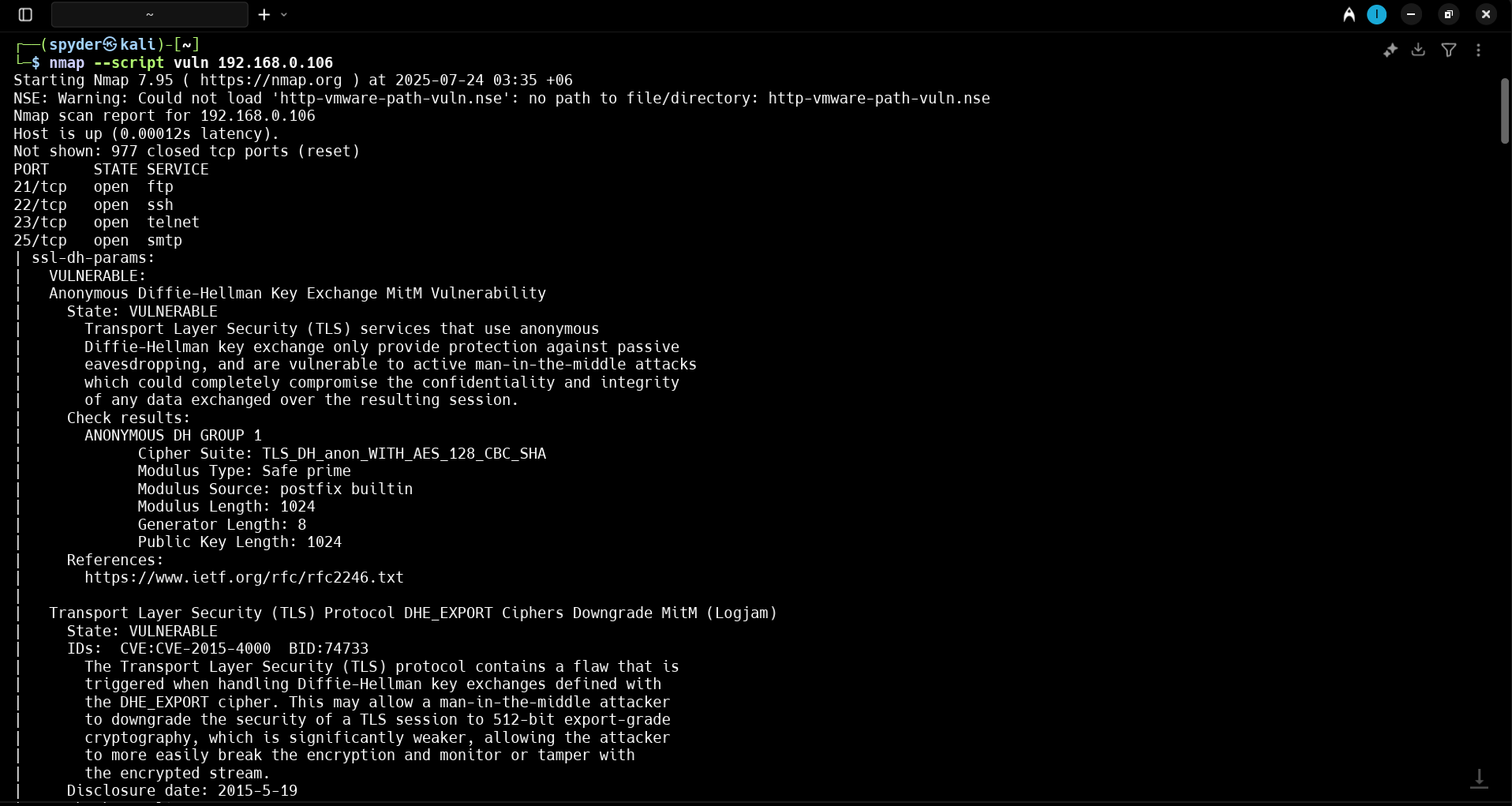
## 

## 



Step 8 : Starting Aggressive Scan with OS , services, Script scan and vulnerabilities finder

**nmap --script vuln **192.168.0.106****

****

****Full Report is here :****

**Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 03:35 +06**

**NSE: Warning: Could not load 'http-vmware-path-vuln.nse': no path to file/directory: http-vmware-path-vuln.nse**

**Nmap scan report for 192.168.0.106**

**Host is up (0.00012s latency).**

**Not shown: 977 closed tcp ports (reset)**

**PORT STATE SERVICE**

**21/tcp open ftp**

**22/tcp open ssh**

**23/tcp open telnet**

**25/tcp open smtp**

**| ssl-dh-params:**

**| VULNERABLE:**

**| Anonymous Diffie-Hellman Key Exchange MitM Vulnerability**

**| State: VULNERABLE**

**| Transport Layer Security (TLS) services that use anonymous**

**| Diffie-Hellman key exchange only provide protection against passive**

**| eavesdropping, and are vulnerable to active man-in-the-middle attacks**

**| which could completely compromise the confidentiality and integrity**

**| of any data exchanged over the resulting session.**

**| Check results:**

**| ANONYMOUS DH GROUP 1**

**| Cipher Suite: TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA**

**| Modulus Type: Safe prime**

**| Modulus Source: postfix builtin**

**| Modulus Length: 1024**

**| Generator Length: 8**

**| Public Key Length: 1024**

**| References:**

**| https://www.ietf.org/rfc/rfc2246.txt**

**|**

**| Transport Layer Security (TLS) Protocol DHE\_EXPORT Ciphers Downgrade MitM (Logjam)**

**| State: VULNERABLE**

**| IDs: CVE:CVE-2015-4000 BID:74733**

**| The Transport Layer Security (TLS) protocol contains a flaw that is**

**| triggered when handling Diffie-Hellman key exchanges defined with**

**| the DHE\_EXPORT cipher. This may allow a man-in-the-middle attacker**

**| to downgrade the security of a TLS session to 512-bit export-grade**

**| cryptography, which is significantly weaker, allowing the attacker**

**| to more easily break the encryption and monitor or tamper with**

**| the encrypted stream.**

**| Disclosure date: 2015-5-19**

**| Check results:**

**| EXPORT-GRADE DH GROUP 1**

**| Cipher Suite: TLS\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA**

**| Modulus Type: Safe prime**

**| Modulus Source: Unknown/Custom-generated**

**| Modulus Length: 512**

**| Generator Length: 8**

**| Public Key Length: 512**

**| References:**

**| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000**

**| https://www.securityfocus.com/bid/74733**

**| https://weakdh.org**

**|**

**| Diffie-Hellman Key Exchange Insufficient Group Strength**

**| State: VULNERABLE**

**| Transport Layer Security (TLS) services that use Diffie-Hellman groups**

**| of insufficient strength, especially those using one of a few commonly**

**| shared groups, may be susceptible to passive eavesdropping attacks.**

**| Check results:**

**| WEAK DH GROUP 1**

**| Cipher Suite: TLS\_DHE\_RSA\_WITH\_DES\_CBC\_SHA**

**| Modulus Type: Safe prime**

**| Modulus Source: postfix builtin**

**| Modulus Length: 1024**

**| Generator Length: 8**

**| Public Key Length: 1024**

**| References:**

**|\_ https://weakdh.org**

**| ssl-poodle:**

**| VULNERABLE:**

**| SSL POODLE information leak**

**| State: VULNERABLE**

**| IDs: CVE:CVE-2014-3566 BID:70574**

**| The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other**

**| products, uses nondeterministic CBC padding, which makes it easier**

**| for man-in-the-middle attackers to obtain cleartext data via a**

**| padding-oracle attack, aka the "POODLE" issue.**

**| Disclosure date: 2014-10-14**

**| Check results:**

**| TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA**

**| References:**

**| https://www.imperialviolet.org/2014/10/14/poodle.html**

**| https://www.openssl.org/~bodo/ssl-poodle.pdf**

**| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566**

**|\_ https://www.securityfocus.com/bid/70574**

**| smtp-vuln-cve2010-4344:**

**|\_ The SMTP server is not Exim: NOT VULNERABLE**

**|\_sslv2-drown: ERROR: Script execution failed (use -d to debug)**

**53/tcp open domain**

**80/tcp open http**

**|\_http-dombased-xss: Couldn't find any DOM based XSS.**

**|\_http-trace: TRACE is enabled**

**| http-sql-injection:**

**| Possible sqli for queries:**

**| http://192.168.0.106:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous**

**| http://192.168.0.106:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=home.php**

**| http://192.168.0.106:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=login.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=home.php**

**| http://192.168.0.106:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=credits.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider**

**| http://192.168.0.106:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider**

**| http://192.168.0.106:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider**

**| http://192.168.0.106:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider**

**| http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?rev2=1.9%27%20OR%20sqlspider&rev1=1.10**

**| http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?rev2=1.9&rev1=1.10%27%20OR%20sqlspider**

**| http://192.168.0.106:80/view/TWiki/TWikiHistory?rev=1.9%27%20OR%20sqlspider**

**| http://192.168.0.106:80/view/TWiki/TWikiHistory?rev=1.8%27%20OR%20sqlspider**

**| http://192.168.0.106:80/oops/TWiki/TWikiHistory?template=oopsrev%27%20OR%20sqlspider&param1=1.10**

**| http://192.168.0.106:80/oops/TWiki/TWikiHistory?template=oopsrev&param1=1.10%27%20OR%20sqlspider**

**| http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?rev2=1.7%27%20OR%20sqlspider&rev1=1.8**

**| http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?rev2=1.7&rev1=1.8%27%20OR%20sqlspider**

**| http://192.168.0.106:80/view/TWiki/TWikiHistory?rev=1.7%27%20OR%20sqlspider**

**| http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?rev2=1.8%27%20OR%20sqlspider&rev1=1.9**

**| http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?rev2=1.8&rev1=1.9%27%20OR%20sqlspider**

**| http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?rev2=1.9%27%20OR%20sqlspider&rev1=1.10**

**| http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?rev2=1.9&rev1=1.10%27%20OR%20sqlspider**

**| http://192.168.0.106:80/view/TWiki/TWikiHistory?rev=1.9%27%20OR%20sqlspider**

**| http://192.168.0.106:80/view/TWiki/TWikiHistory?rev=1.8%27%20OR%20sqlspider**

**| http://192.168.0.106:80/oops/TWiki/TWikiHistory?template=oopsrev%27%20OR%20sqlspider&param1=1.10**

**| http://192.168.0.106:80/oops/TWiki/TWikiHistory?template=oopsrev&param1=1.10%27%20OR%20sqlspider**

**| http://192.168.0.106:80/view/TWiki/TWikiHistory?rev=1.7%27%20OR%20sqlspider**

**| http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?rev2=1.7%27%20OR%20sqlspider&rev1=1.8**

**| http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?rev2=1.7&rev1=1.8%27%20OR%20sqlspider**

**| http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?rev2=1.8%27%20OR%20sqlspider&rev1=1.9**

**| http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?rev2=1.8&rev1=1.9%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous**

**| http://192.168.0.106:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=login.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=credits.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=rene-magritte.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous**

**| http://192.168.0.106:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=login.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=credits.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider**

**| http://192.168.0.106:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider**

**|\_ http://192.168.0.106:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider**

**| http-csrf:**

**| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.0.106**

**| Found the following possible CSRF vulnerabilities:**

**|**

**| Path: http://192.168.0.106:80/dvwa/**

**| Form id:**

**| Form action: login.php**

**|**

**| Path: http://192.168.0.106:80/dvwa/login.php**

**| Form id:**

**| Form action: login.php**

**|**

**| Path: http://192.168.0.106:80/twiki/TWikiDocumentation.html**

**| Form id:**

**| Form action: http://TWiki.org/cgi-bin/passwd/TWiki/WebHome**

**|**

**| Path: http://192.168.0.106:80/twiki/TWikiDocumentation.html**

**| Form id:**

**| Form action: http://TWiki.org/cgi-bin/passwd/Main/WebHome**

**|**

**| Path: http://192.168.0.106:80/twiki/TWikiDocumentation.html**

**| Form id:**

**| Form action: http://TWiki.org/cgi-bin/edit/TWiki/**

**|**

**| Path: http://192.168.0.106:80/twiki/TWikiDocumentation.html**

**| Form id:**

**| Form action: http://TWiki.org/cgi-bin/view/TWiki/TWikiSkins**

**|**

**| Path: http://192.168.0.106:80/twiki/TWikiDocumentation.html**

**| Form id:**

**|\_ Form action: http://TWiki.org/cgi-bin/manage/TWiki/ManagingWebs**

**|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.**

**| http-fileupload-exploiter:**

**|**

**|\_ Couldn't find a file-type field.**

**|\_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)**

**| http-enum:**

**| /tikiwiki/: Tikiwiki**

**| /test/: Test page**

**| /phpinfo.php: Possible information file**

**| /phpMyAdmin/: phpMyAdmin**

**| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'**

**| /icons/: Potentially interesting folder w/ directory listing**

**|\_ /index/: Potentially interesting folder**

**111/tcp open rpcbind**

**139/tcp open netbios-ssn**

**445/tcp open microsoft-ds**

**512/tcp open exec**

**513/tcp open login**

**514/tcp open shell**

**1099/tcp open rmiregistry**

**| rmi-vuln-classloader:**

**| VULNERABLE:**

**| RMI registry default configuration remote code execution vulnerability**

**| State: VULNERABLE**

**| Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.**

**|**

**| References:**

**|\_ https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java\_rmi\_server.rb**

**1524/tcp open ingreslock**

**2049/tcp open nfs**

**2121/tcp open ccproxy-ftp**

**3306/tcp open mysql**

**|\_ssl-ccs-injection: No reply from server (TIMEOUT)**

**5432/tcp open postgresql**

**| ssl-poodle:**

**| VULNERABLE:**

**| SSL POODLE information leak**

**| State: VULNERABLE**

**| IDs: CVE:CVE-2014-3566 BID:70574**

**| The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other**

**| products, uses nondeterministic CBC padding, which makes it easier**

**| for man-in-the-middle attackers to obtain cleartext data via a**

**| padding-oracle attack, aka the "POODLE" issue.**

**| Disclosure date: 2014-10-14**

**| Check results:**

**| TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA**

**| References:**

**| https://www.imperialviolet.org/2014/10/14/poodle.html**

**| https://www.openssl.org/~bodo/ssl-poodle.pdf**

**| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566**

**|\_ https://www.securityfocus.com/bid/70574**

**| ssl-ccs-injection:**

**| VULNERABLE:**

**| SSL/TLS MITM vulnerability (CCS Injection)**

**| State: VULNERABLE**

**| Risk factor: High**

**| OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h**

**| does not properly restrict processing of ChangeCipherSpec messages,**

**| which allows man-in-the-middle attackers to trigger use of a zero**

**| length master key in certain OpenSSL-to-OpenSSL communications, and**

**| consequently hijack sessions or obtain sensitive information, via**

**| a crafted TLS handshake, aka the "CCS Injection" vulnerability.**

**|**

**| References:**

**| http://www.openssl.org/news/secadv\_20140605.txt**

**| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224**

**|\_ http://www.cvedetails.com/cve/2014-0224**

**| ssl-dh-params:**

**| VULNERABLE:**

**| Diffie-Hellman Key Exchange Insufficient Group Strength**

**| State: VULNERABLE**

**| Transport Layer Security (TLS) services that use Diffie-Hellman groups**

**| of insufficient strength, especially those using one of a few commonly**

**| shared groups, may be susceptible to passive eavesdropping attacks.**

**| Check results:**

**| WEAK DH GROUP 1**

**| Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA**

**| Modulus Type: Safe prime**

**| Modulus Source: Unknown/Custom-generated**

**| Modulus Length: 1024**

**| Generator Length: 8**

**| Public Key Length: 1024**

**| References:**

**|\_ https://weakdh.org**

**5900/tcp open vnc**

**6000/tcp open X11**

**6667/tcp open irc**

**|\_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/fulldisclosure/2010/Jun/277**

**8009/tcp open ajp13**

**8180/tcp open unknown**

**| http-cookie-flags:**

**| /admin/:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/index.html:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/login.html:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/admin.html:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/account.html:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/admin\_login.html:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/home.html:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/admin-login.html:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/adminLogin.html:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/controlpanel.html:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/cp.html:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/index.jsp:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/login.jsp:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/admin.jsp:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/home.jsp:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/controlpanel.jsp:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/admin-login.jsp:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/cp.jsp:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/account.jsp:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/admin\_login.jsp:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/adminLogin.jsp:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/includes/FCKeditor/editor/filemanager/upload/test.html:**

**| JSESSIONID:**

**| httponly flag not set**

**| /admin/jscript/upload.html:**

**| JSESSIONID:**

**|\_ httponly flag not set**

**| http-slowloris-check:**

**| VULNERABLE:**

**| Slowloris DOS attack**

**| State: LIKELY VULNERABLE**

**| IDs: CVE:CVE-2007-6750**

**| Slowloris tries to keep many connections to the target web server open and hold**

**| them open as long as possible. It accomplishes this by opening connections to**

**| the target web server and sending a partial request. By doing so, it starves**

**| the http server's resources causing Denial Of Service.**

**|**

**| Disclosure date: 2009-09-17**

**| References:**

**| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750**

**|\_ http://ha.ckers.org/slowloris/**

**| http-enum:**

**| /admin/: Possible admin folder**

**| /admin/index.html: Possible admin folder**

**| /admin/login.html: Possible admin folder**

**| /admin/admin.html: Possible admin folder**

**| /admin/account.html: Possible admin folder**

**| /admin/admin\_login.html: Possible admin folder**

**| /admin/home.html: Possible admin folder**

**| /admin/admin-login.html: Possible admin folder**

**| /admin/adminLogin.html: Possible admin folder**

**| /admin/controlpanel.html: Possible admin folder**

**| /admin/cp.html: Possible admin folder**

**| /admin/index.jsp: Possible admin folder**

**| /admin/login.jsp: Possible admin folder**

**| /admin/admin.jsp: Possible admin folder**

**| /admin/home.jsp: Possible admin folder**

**| /admin/controlpanel.jsp: Possible admin folder**

**| /admin/admin-login.jsp: Possible admin folder**

**| /admin/cp.jsp: Possible admin folder**

**| /admin/account.jsp: Possible admin folder**

**| /admin/admin\_login.jsp: Possible admin folder**

**| /admin/adminLogin.jsp: Possible admin folder**

**| /manager/html/upload: Apache Tomcat (401 Unauthorized)**

**| /manager/html: Apache Tomcat (401 Unauthorized)**

**| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload**

**| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload**

**| /admin/jscript/upload.html: Lizard Cart/Remote File upload**

**|\_ /webdav/: Potentially interesting folder**

**MAC Address: 08:00:27:37:45:88 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)**

**Host script results:**

**|\_smb-vuln-ms10-054: false**

**|\_smb-vuln-ms10-061: false**

**|\_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)**

**Nmap done: 1 IP address (1 host up) scanned in 334.17 seconds**

****Summarized List of all the ssl-dh-params Vulnerabilities :****

1. **Anonymous Diffie-Hellman Key Exchange MitM Vulnerability :**

Check results:

ANONYMOUS DH GROUP 1

Cipher Suite: TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA

Modulus Type: Safe prime

Modulus Source: postfix builtin

Modulus Length: 1024

Generator Length: 8

Public Key Length: 1024

1. Transport Layer Security (TLS) Protocol DHE\_EXPORT Ciphers Downgrade MitM (Logjam)

IDs: CVE:CVE-2015-4s000 BID:74733

Check results:

EXPORT-GRADE DH GROUP 1

Cipher Suite: TLS\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA

Modulus Type: Safe prime

Modulus Source: Unknown/Custom-generated

Modulus Length: 512

Generator Length: 8

Public Key Length: 512

1. Diffie-Hellman Key Exchange Insufficient Group Strength

Check results:

WEAK DH GROUP 1

Cipher Suite: TLS\_DHE\_RSA\_WITH\_DES\_CBC\_SHA

Modulus Type: Safe prime

Modulus Source: postfix builtin

Modulus Length: 1024

Generator Length: 8

Public Key Length: 1024

****Summarized List of all the ssl-poodle Vulnerabilities :****

1. SSL POODLE information leak

IDs: CVE:CVE-2014-3566 BID:70574

Check results:

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

****Summarized List of all the http-slowloris-check Vulnerabilities :****

1. Slowloris DOS attack

IDs: CVE:CVE-2007-6750

**Same as we can find Vulnerabilities using Zenmap :**

