**STEP 1 : INSTALL NMAP FROM THE BROWSER**

**STEP 1: OPEN COMMAND PROMPT OF MY PC AND PUT MY LOCAL PC COMMAND**

**C:\Users\Ayan Sable>ipconfig**

**Windows IP Configuration**

**Wireless LAN adapter Wi-Fi 2:**

**Media State . . . . . . . . . . . : Media disconnected**

**Connection-specific DNS Suffix . :**

**Wireless LAN adapter Wi-Fi 4:**

**Media State . . . . . . . . . . . : Media disconnected**

**Connection-specific DNS Suffix . :**

**Wireless LAN adapter Wi-Fi:**

**Connection-specific DNS Suffix . :**

**Link-local IPv6 Address . . . . . : fe80::aa52:472:aac:5b7a%13**

**IPv4 Address. . . . . . . . . . . : 192.168.0.104**

**Subnet Mask . . . . . . . . . . . : 255.255.255.0**

**Default Gateway . . . . . . . . . : 192.168.0.1**

**STEP 3:ANALYZE MY LOCAL COMMAND ON NMAP AND SCAN THEN THE OUTPUT COMES..**

**A screenshot of a computer program

AI-generated content may be incorrect.**

**STEP 4: I HAVE SCAN MY LOCAL WINDOWS IP TO PERFORM TCP SYN STEALTH SCAN WITH (nmap -sS 192.168.0.104)**

**A screenshot of a computer

AI-generated content may be incorrect.**

**ITS SHOWS ME THE AND UNDERSTAND THE OUTPUT**

1. **SYN-ACK =Port is open**
2. **RST= Port is closed**
3. **No Respense :Port is filtered (means protected by firewall)**

**STEP 5: I HAVE USE A COMMAND FOR ANY SECURITY DETECTION MY LOCAL HOST (nmap -A 192.168.0.104) IT GIVES A DETAILS FINGERPRINT OF THE TARGET HOST**

**A screenshot of a computer

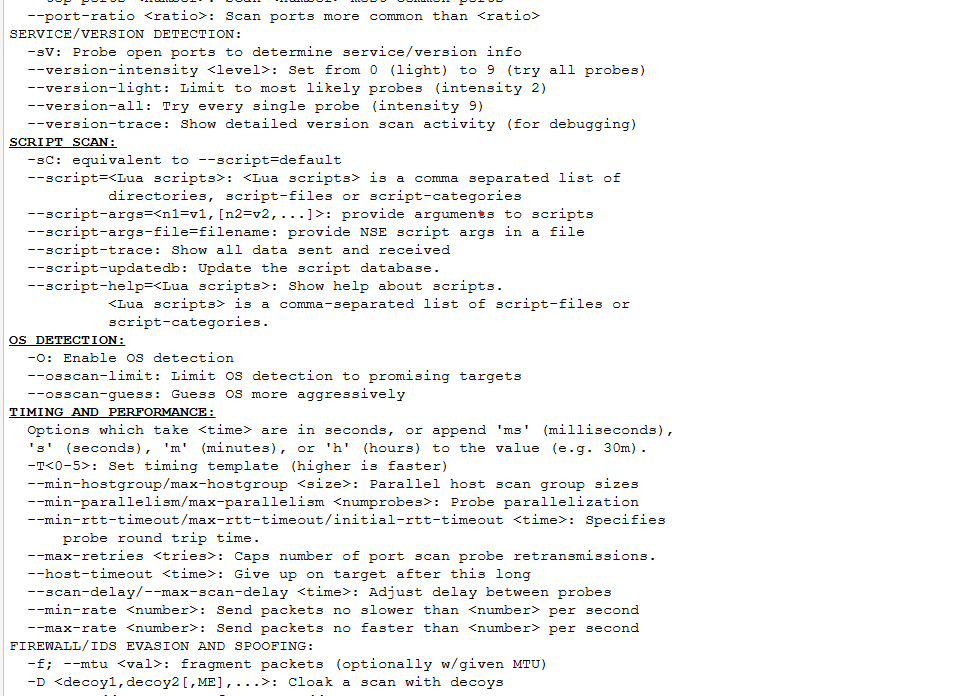
AI-generated content may be incorrect.**

**ITS SHOW THE VULNERABILITY ,MISCONFIGURATIONS AND SSL INFO.**

**STEP 6: I HAVE JUST USE PING COMMAND FOR TAKING RESPONSE FROM MY PC (nmap -sn 192.168.0.104)**

****

**STEP 7 :I HAVE USE THE COMMAND TO CHECK THE SERVICE VERSION (nmap -sV 192.168.0.104)**

****

**STEP 8:SCANNING A SPECIFIC PORT I HAVE SCAN PORT NUMBER 22 (nmap -p 22 192.168.0.104) IT STATE THAT’S IT PORT IS CLOSED OF MY OS**

**A screenshot of a computer

AI-generated content may be incorrect.**