TASK 1

Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-04 20:32 +0530

NSE: Loaded 158 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 20:32

Completed NSE at 20:32, 0.00s elapsed

Initiating NSE at 20:32

Completed NSE at 20:32, 0.00s elapsed

Initiating NSE at 20:32

Completed NSE at 20:32, 0.00s elapsed

Initiating Parallel DNS resolution of 1 host. at 20:32

Completed Parallel DNS resolution of 1 host. at 20:32, 0.51s elapsed

Initiating System DNS resolution of 1 host. at 20:32

Completed System DNS resolution of 1 host. at 20:32, 2.73s elapsed

Failed to resolve "nmap".

Initiating Parallel DNS resolution of 1 host. at 20:32

Completed Parallel DNS resolution of 1 host. at 20:32, 0.50s elapsed

Initiating SYN Stealth Scan at 20:32

Scanning 172.21.241.133 [1000 ports]

Discovered open port 445/tcp on 172.21.241.133

Discovered open port 139/tcp on 172.21.241.133

Discovered open port 135/tcp on 172.21.241.133

Discovered open port 16992/tcp on 172.21.241.133

Discovered open port 8089/tcp on 172.21.241.133

Discovered open port 8000/tcp on 172.21.241.133

Completed SYN Stealth Scan at 20:32, 0.08s elapsed (1000 total ports)

Initiating Service scan at 20:32

Scanning 6 services on 172.21.241.133

Completed Service scan at 20:32, 29.67s elapsed (6 services on 1 host)

Initiating OS detection (try #1) against 172.21.241.133

NSE: Script scanning 172.21.241.133.

Initiating NSE at 20:32

Completed NSE at 20:32, 14.91s elapsed

Initiating NSE at 20:32

Completed NSE at 20:32, 0.09s elapsed

Initiating NSE at 20:32

Completed NSE at 20:32, 0.00s elapsed

Nmap scan report for 172.21.241.133

Host is up (0.00048s latency).

Not shown: 994 closed tcp ports (reset)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

8000/tcp open http Splunkd httpd

|\_http-server-header: Splunkd

|\_http-favicon: Unknown favicon MD5: E60C968E8FF3CC2F4FB869588E83AFC6

| http-methods:

|\_ Supported Methods: GET HEAD POST OPTIONS

| http-robots.txt: 1 disallowed entry

|\_/

| http-title: Site doesn't have a title (text/html; charset=UTF-8).

|\_Requested resource was http://172.21.241.133:8000/en-US/account/login?return\_to=%2Fen-US%2F

8089/tcp open ssl/http Splunkd httpd

| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser

| Issuer: commonName=SplunkCommonCA/organizationName=Splunk/stateOrProvinceName=CA/countryName=US

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2025-07-14T06:21:08

| Not valid after: 2028-07-13T06:21:08

| MD5: 3a72 b77c 4b96 33bb c781 9f63 4e01 9bf1

| SHA-1: bce1 f56b 10c6 c8e4 8e99 1049 83aa 5a2c e5df 3245

|\_SHA-256: bb13 487f c6be fc47 f823 a393 0fd7 5a1f 6cbe cc04 beb3 2372 e172 ac4e 394d 909e

|\_http-server-header: Splunkd

|\_http-title: splunkd

| http-methods:

|\_ Supported Methods: GET HEAD OPTIONS

| http-robots.txt: 1 disallowed entry

|\_/

16992/tcp open http Intel Active Management Technology User Notification Service httpd 12.0.96.2562

|\_http-server-header: Intel(R) Active Management Technology 12.0.96.2562

| http-title: Intel&reg; Active Management Technology

|\_Requested resource was /logon.htm

| http-methods:

|\_ Supported Methods: GET HEAD POST

Device type: general purpose

Running: Microsoft Windows 10|11

OS CPE: cpe:/o:microsoft:windows\_10 cpe:/o:microsoft:windows\_11

OS details: Microsoft Windows 10 1607 - 11 23H2

Uptime guess: 0.096 days (since Mon Aug 4 18:14:22 2025)

Network Distance: 0 hops

TCP Sequence Prediction: Difficulty=261 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/h:intel:active\_management\_technology:12.0.96.2562

Host script results:

| smb2-time:

| date: 2025-08-04T15:02:45

|\_ start\_date: N/A

| smb2-security-mode:

| 3.1.1:

|\_ Message signing enabled but not required

NSE: Script Post-scanning.

Initiating NSE at 20:32

Completed NSE at 20:32, 0.00s elapsed

Initiating NSE at 20:32

Completed NSE at 20:32, 0.00s elapsed

Initiating NSE at 20:32

Completed NSE at 20:32, 0.00s elapsed

Read data files from: C:\Program Files (x86)\Nmap

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 58.63 seconds

Raw packets sent: 1016 (45.418KB) | Rcvd: 2046 (87.346KB)