

PORT	STATE	SERVICE
135 / TCP	Open	MSRPC
139 / TCP	Open /	NetBios-ssn
445 / TCP	Open /	Microsoft-ds
554 / TCP	Open /	RTSP
2869 / TCP	Open /	HTTP
3389 / TCP	Open /	SSL / Ms-wbt-server
5357 / TCP	Open	HTTP
8089 / TCP	Open	SSL / HTTP

```
(sierra@kali)-[~/Downloads]
$ nmap -sV 10.0.0.74
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-22 13:15 EDT
Nmap scan report for 10.0.0.74
Host is up (0.10s latency).
Not shown: 986 closed tcp ports (conn-refused)
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     Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp    open  rtsp?            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
2869/tcp   open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp   open  ssl/ms-wbt-server? Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp   open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8089/tcp   open  ssl/http         Splunkd httpd
10243/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp  open  msrpc            Microsoft Windows RPC
49153/tcp  open  msrpc            Microsoft Windows RPC
49154/tcp  open  msrpc            Microsoft Windows RPC
49155/tcp  open  msrpc            Microsoft Windows RPC
49163/tcp  open  msrpc            Microsoft Windows RPC
Service Info: Host: RISK-ANALYST1; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit.
Nmap done: 1 IP address (1 host up) scanned in 142.40 seconds
```

```

(kali@kali)-[~]
$ nmap -sV --script vuln 10.0.0.74
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-19 18:15 EDT
Stats: 0:07:57 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.89% done; ETC: 18:23 (0:00:00 remaining)
Nmap scan report for 10.0.0.74
Host is up (0.024s latency).
Not shown: 986 closed tcp ports (conn-refused)
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       Microsoft Windows 7 - 10 microsoft-ds (workgroup: OUP)
554/tcp    open  rtsp              RealTime Streaming Protocol
2869/tcp   open  http              Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
3389/tcp   open  ssl/ms-wbt-server?
| 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_128_CBC_SHA
|       Modulus Type: Safe prime
|       Modulus Source: RFC2409/Oakley Group 2
|       Modulus Length: 1024
|       Generator Length: 1024
|       Public Key Length: 1024
|   References:
|     https://weakdh.org
5357/tcp   open  http              Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-server-header: Microsoft-HTTPAPI/2.0
8089/tcp   open  ssl/http          Splunkd httpd
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-server-header: Splunkd
| http-slowloris-check:

```

```

|_ http-server-header: Splunkd
| 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/
10243/tcp  open  http              Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp  open  msrpc             Microsoft Windows RPC
49153/tcp  open  msrpc             Microsoft Windows RPC
49154/tcp  open  msrpc             Microsoft Windows RPC
49155/tcp  open  msrpc             Microsoft Windows RPC
49163/tcp  open  msrpc             Microsoft Windows RPC
Service Info: Host: RISK-ANALYST1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

```

```

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 406.71 seconds

```