

```
└──(root@kali) - [~]
└──# nmap -sC -sV -O -p- $w2k8 > nmap_resurt_w2k8.txt
└──(root@kali) - [~]
└──# cat nmap_resurt_w2k8.txt Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 19:36 EST
```

Nmap scan report for 10.0.0.31

Host is up (0.00032s latency).

Not shown: 65514 filtered tcp ports (no-response)

| PORT | STATE | SERVICE | VERSION |
|------|-------|---------|---------|
|------|-------|---------|---------|

| | | | |
|--------|------|-----|----------------|
| 21/tcp | open | ftp | Microsoft ftpd |
|--------|------|-----|----------------|

| ftp-syst:

|_ SYST: Windows_NT

| | | | |
|--------|------|-----|----------------------------|
| 22/tcp | open | ssh | OpenSSH 7.1 (protocol 2.0) |
|--------|------|-----|----------------------------|

| ssh-hostkey:

| 2048 ab:20:08:36:e3:ef:27:0c:90:fa:15:67:f3:f5:5b:db (RSA)

|_ 521 07:70:d3:4f:f0:80:2d:b4:bb:d6:42:5e:8c:02:4e:09 (ECDSA)

| | | | |
|--------|------|------|-------------------------|
| 80/tcp | open | http | Microsoft IIS httpd 7.5 |
|--------|------|------|-------------------------|

| http-methods:

|_ Potentially risky methods: TRACE

|_ http-title: Site doesn't have a title (text/html).

|_ http-server-header: Microsoft-IIS/7.5

| | | | |
|---------|------|-------|-----------------------|
| 135/tcp | open | msrpc | Microsoft Windows RPC |
|---------|------|-------|-----------------------|

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

| | | | |
|---------|------|--------------|---|
| 445/tcp | open | microsoft-ds | Windows Server 2008 R2 Standard 7601 Service Pack 1 |
|---------|------|--------------|---|

| | | | |
|----------|------|----------|----------|
| 1617/tcp | open | java-rmi | Java RMI |
|----------|------|----------|----------|

| rmi-dumpregistry:

| jmxrmi

| javax.management.remote.rmi.RMIServerImpl_Stub

| @10.0.0.31:49239

| extends

| java.rmi.server.RemoteStub

| extends

|_ java.rmi.server.RemoteObject

| | | | |
|----------|------|------|---|
| 3000/tcp | open | http | WEBrick httpd 1.3.1 (Ruby 2.3.3 (2016-11-21)) |
|----------|------|------|---|

|_ http-server-header: WEBrick/1.3.1 (Ruby/2.3.3/2016-11-21)

|_ http-robots.txt: 1 disallowed entry

|_ /

|_ http-title: Ruby on Rails: Welcome aboard

| | | | |
|----------|------|-------|--|
| 3306/tcp | open | mysql | MySQL (blocked - too many connection errors) |
|----------|------|-------|--|

| | | | |
|----------|------|----------|---|
| 4848/tcp | open | ssl/http | Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8) |
|----------|------|----------|---|

|_ http-server-header: GlassFish Server Open Source Edition 4.0

|_ ssl-cert: Subject: commonName=localhost/organizationName=Oracle

Corporation/stateOrProvinceName=California/countryName=US

|_ Not valid before: 2013-05-15T05:33:38

|_ Not valid after: 2023-05-13T05:33:38

|_ ssl-date: 2025-11-10T17:39:37+00:00; +17h00m01s from scanner time.

|_ http-title: Login

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found

8022/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache-Coyote/1.1
| http-methods:
|_ Potentially risky methods: PUT DELETE

8080/tcp open http Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
|_http-title: GlassFish Server - Server Running
| http-methods:
|_ Potentially risky methods: PUT DELETE TRACE
|_http-server-header: GlassFish Server Open Source Edition 4.0
|_http-open-proxy: Proxy might be redirecting requests

8282/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/8.0.33
|_http-favicon: Apache Tomcat

8484/tcp open http Jetty winstone-2.8
|_http-server-header: Jetty(winstone-2.8)
| http-robots.txt: 1 disallowed entry
|_
|_http-title: Dashboard [Jenkins]

8585/tcp open http Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
|_http-server-header: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
|_http-title: WAMPSEVER Homepage

9200/tcp open http Elasticsearch REST API 1.1.1 (name: Yondu; Lucene 4.7)
|_http-cors: HEAD GET POST PUT DELETE OPTIONS
|_http-title: Site doesn't have a title (application/json; charset=UTF-8).

49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49239/tcp open java-rmi Java RMI
49240/tcp open tcpwrapped

MAC Address: 00:0C:29:E0:CA:49 (VMware)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: phone
Running: Microsoft Windows Phone
OS CPE: cpe:/o:microsoft:windows
OS details: Microsoft Windows Phone 7.5 or 8.0
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
| 2:1:0:
|_ Message signing enabled but not required
| smb-os-discovery:
| OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2

Standard 6.1)

| OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
| Computer name: metasploitable3
| NetBIOS computer name: METASPLOITABLE3Wx00
| Workgroup: WORKGROUPWx00
|_ System time: 2025-11-10T09:39:02-08:00
| smb2-time:
| date: 2025-11-10T17:38:58
|_ start_date: 2025-11-10T16:55:56
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 19h00m03s, deviation: 4h00m05s, median: 17h00m00s

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 210.83 seconds