```
<get_results_response status="200" status_text="OK"><result id="9f54137f-f995-4596-8843-6eed51a1d854"><name>
2</name></owner><modification_time>2025-08-07T13:20:35Z</modification_time><comment></comment><creatio
b990da552a56"/><task id="17cb935e-cb10-4814-9191-ee321e1acd66"><name>Localhost Scan</name></task><host
</hostname></host><port>135/tcp</port><nvt oid="1.3.6.1.4.1.25623.1.0.10736"><type>nvt</type><name>DCE/RP
ss_base>5.0</cvss_base><severities score="5.0"><severity type="cvss_base_v2"><origin></origin><date>2017-01-12
alue></severity></severities><tags>cvss_base_vector=AV:N/AC:L/Au:N/C:P/I:N/A:N|summary=Distributed Computing
  on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.|insight=|aff
  about the remote host.|solution=Filter incoming traffic to this ports.|vuldetect=|solution_type=Mitigation</tags><s
</solution></nvt><scan_nvt_version>2022-06-03T10:17:07Z</scan_nvt_version><threat>Medium</threat><severity>
s the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 49664/tcp

    UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
    Endpoint: ncacn_ip_tcp:192.168.56.1[49664]
    Named pipe : lsass
    Win32 service or process : lsass.exe
    Description : SAM access

    UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
    Endpoint: ncacn_ip_tcp:192.168.56.1[49664]
    Annotation: Ngc Pop Key Service

    UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
    Endpoint: ncacn_ip_tcp:192.168.56.1[49664]
    Annotation: Ngc Pop Key Service

    UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
    Endpoint: ncacn_ip_tcp:192.168.56.1[49664]
    Annotation: KeyIso

Port: 49665/tcp

    UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
    Endpoint: ncacn_ip_tcp:192.168.56.1[49665]

Port: 49666/tcp

    UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
    Endpoint: ncacn_ip_tcp:192.168.56.1[49666]
    Annotation: Windows Event Log

Port: 49667/tcp

    UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
    Endpoint: ncacn_ip_tcp:192.168.56.1[49667]

    UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
    Endpoint: ncacn_ip_tcp:192.168.56.1[49667]

Port: 49668/tcp

    UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
    Endpoint: ncacn_ip_tcp:192.168.56.1[49668]

    UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
    Endpoint: ncacn_ip_tcp:192.168.56.1[49668]
    Named pipe : spoolss
    Win32 service or process : spoolsv.exe
    Description : Spooler service
```

```
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:192.168.56.1[49668]

     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:192.168.56.1[49668]

     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:192.168.56.1[49668]

Port: 49721/tcp

     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.56.1[49721]

Note: DCE/RPC or MSRPC services running on this host locally were identified. Reporting this list is not enabled by de
pt preferences to enable this reporting.
</description><original_threat>Medium</original_threat><original_severity>5</original_severity><compliance>unde
0923a"><name>SMB/CIFS Server Detection</name><owner><name>admin2</name></owner><modification_time>
7T13:18:40Z</creation_time><report id="d057bfbe-4ae6-4d2d-b173-b990da552a56"/><task id="17cb935e-cb10-481
set asset_id="459291f2-4d4d-4fc9-83e9-fb610ad0de35"/><hostname></hostname></host><port>445/tcp</port><nv
ection</name><family>Service detection</family><cvss_base>0.0</cvss_base><severities score="0.0"><severity type
re>0.0</score><value>AV:N/AC:L/Au:N/C:N/I:N/A:N</value></severity></severities><tags>cvss_base_vector=AV:N/AC
 are open and
  if they are running a CIFS/SMB server.|insight=|affected=|impact=|solution=|vuldetect=|solution_type=</tags><sc
0Z</scan_nvt_version><threat>Log</threat><severity>0.0</severity><qod><value>80</value><type></type></qod><
</description><original_threat>Log</original_threat><original_severity>0</original_severity><compliance>undefined
e1"><name>SMB/CIFS Server Detection</name><owner><name>admin2</name></owner><modification_time>202
3:18:40Z</creation_time><report id="d057bfbe-4ae6-4d2d-b173-b990da552a56"/><task id="17cb935e-cb10-4814-91
 asset_id="459291f2-4d4d-4fc9-83e9-fb610ad0de35"/><hostname></hostname></host><port>139/tcp</port><nvt o
ion</name><family>Service detection</family><cvss_base>0.0</cvss_base><severities score="0.0"><severity type="
0.0</score><value>AV:N/AC:L/Au:N/C:N/I:N/A:N</value></severity></severities><tags>cvss_base_vector=AV:N/AC:L/
e open and
  if they are running a CIFS/SMB server.|insight=|affected=|impact=|solution=|vuldetect=|solution_type=</tags><sc
0Z</scan_nvt_version><threat>Log</threat><severity>0.0</severity><qod><value>80</value><type></type></qod><
</description><original_threat>Log</original_threat><original_severity>0</original_severity><compliance>undefined
56"><name>OS Detection Consolidation and Reporting</name><owner><name>admin2</name></owner><modific
me>2025-08-07T13:19:25Z</creation_time><report id="d057bfbe-4ae6-4d2d-b173-b990da552a56"/><task id="17cb
.168.56.1<asset asset_id="459291f2-4d4d-4fc9-83e9-fb610ad0de35"/><hostname></hostname></host><port>gener
 Detection Consolidation and Reporting</name><family>Product detection</family><cvss_base>0.0</cvss_base><se
>2016-02-19T10:19:54Z</date><score>0.0</score><value>AV:N/AC:L/Au:N/C:N/I:N/A:N</value></severity></severitie
consolidates the OS information detected by several
  VTs and tries to find the best matching OS.

  Furthermore it reports all previously collected information leading to this best matching OS. It
  also reports possible additional information which might help to improve the OS detection.

  If any of this information is wrong or could be improved please consider to report these to the
  referenced community forum.|insight=|affected=|impact=|solution=|vuldetect=|solution_type=</tags><solution t
/c/vulnerability-tests/7"/></refs></nvt><scan_nvt_version>2025-08-01T15:45:49Z</scan_nvt_version><threat>Log</t
><description>Best matching OS:

OS:           Microsoft Windows
CPE:          cpe:/o:microsoft:windows
Found by VT:  1.3.6.1.4.1.25623.1.0.108044 (DCE/RPC and MSRPC Services Enumeration)
Concluded from DCE/RPC and MSRPC Services Enumeration on port 135/tcp
Setting key &quot;Host/runs_windows&quot; based on this information
</description><original_threat>Log</original_threat><original_severity>0</original_severity><compliance>undefined
38"><name>SMB Remote Version Detection</name><owner><name>admin2</name></owner><modification_time>
7T13:19:45Z</creation_time><report id="d057bfbe-4ae6-4d2d-b173-b990da552a56"/><task id="17cb935e-cb10-481
```

set asset_id="459291f2-4d4d-4fc9-83e9-fb610ad0de35"/><hostname></hostname></host><port>445/tcp</port><nv
 Detection</name><family>Service detection</family><cvss_base>0.0</cvss_base><severities score="0.0"><severity
<score>0.0</score><value>AV:N/AC:L/Au:N/C:N/I:N/A:N</value></severity></severities><tags>cvss_base_vector=AV:

  This script sends SMB Negotiation request and try to get the version from the
  response.|insight=|affected=|impact=|solution=|vuldetect=|solution_type=</tags><solution type=''></solution></
Log</threat><severity>0.0</severity><qod><value>80</value><type></type></qod><description>SMBv2 and SMBv3
</description><original_threat>Log</original_threat><original_severity>0</original_severity><compliance>undefined
53"><name>Traceroute</name><owner><name>admin2</name></owner><modification_time>2025-08-07T13:19:4
ion_time><report id="d057bfbe-4ae6-4d2d-b173-b990da552a56"/><task id="17cb935e-cb10-4814-9191-ee321e1acd
91f2-4d4d-4fc9-83e9-fb610ad0de35"/><hostname></hostname></host><port>general/tcp</port><nvt oid="1.3.6.1.4
/family><cvss_base>0.0</cvss_base><severities score="0.0"><severity type="cvss_base_v2"><origin></origin><date>
/I:N/A:N</value></severity></severities><tags>cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:N|summary=Collect info
  network distance between the scanner host and the target host.|insight=For internal networks, the distances are u
  small, often less than 4 hosts between scanner and target. For public targets the
  distance is greater and might be 10 hosts or more.|affected=|impact=|solution=|vuldetect=A combination of the p
  to determine the route. This method is applicable for IPv4 only and it is also known as
  &apos;traceroute&apos;.|solution_type=</tags><solution type=''></solution></nvt><scan_nvt_version>2022-10-17
y><qod><value>80</value><type></type></qod><description>Network route from scanner (10.0.2.15) to target (192

10.0.2.15
192.168.56.1

Network distance between scanner and target: 2
</description><original_threat>Log</original_threat><original_severity>0</original_severity><compliance>undefined
c7"><name>Unknown OS and Service Banner Reporting</name><owner><name>admin2</name></owner><modifi
e>2025-08-07T13:21:05Z</creation_time><report id="d057bfbe-4ae6-4d2d-b173-b990da552a56"/><task id="17cb93
168.56.1<asset asset_id="459291f2-4d4d-4fc9-83e9-fb610ad0de35"/><hostname></hostname></host><port>6850/t
n OS and Service Banner Reporting</name><family>Service detection</family><cvss_base>0.0</cvss_base><severiti
-05-02T08:53:41Z</date><score>0.0</score><value>AV:N/AC:L/Au:N/C:N/I:N/A:N</value></severity></severities><ta
tes and reports the information collected by
  the following VTs:

  - Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)

  - Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)

  - Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)

  - OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

  If you know any of the information reported here, please send the full output to
  the referenced community forum.|insight=|affected=|impact=|solution=|vuldetect=|solution_type=</tags><soluti
.net/c/vulnerability-tests/7"/></refs></nvt><scan_nvt_version>2023-06-22T10:34:15Z</scan_nvt_version><threat>Lo
/qod><description>Nmap service detection (unknown) result for this port: iccrushmore

This is a guess. A confident identification of the service was not possible.

Hint: If you&apos;re running a recent nmap version try to run nmap with the following command: &apos;nmap -sV -
int to the nmap database.
</description><original_threat>Log</original_threat><original_severity>0</original_severity><compliance>undefined
12"><name>Unknown OS and Service Banner Reporting</name><owner><name>admin2</name></owner><modifi
e>2025-08-07T13:21:05Z</creation_time><report id="d057bfbe-4ae6-4d2d-b173-b990da552a56"/><task id="17cb93
168.56.1<asset asset_id="459291f2-4d4d-4fc9-83e9-fb610ad0de35"/><hostname></hostname></host><port>7680/t
n OS and Service Banner Reporting</name><family>Service detection</family><cvss_base>0.0</cvss_base><severiti
-05-02T08:53:41Z</date><score>0.0</score><value>AV:N/AC:L/Au:N/C:N/I:N/A:N</value></severity></severities><ta
tes and reports the information collected by
  the following VTs:

  - Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)

```
  - Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)

  - Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)

  - OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

  If you know any of the information reported here, please send the full output to
  the referenced community forum.|insight=|affected=|impact=|solution=|vuldetect=|solution_type=</tags><solut
.net/c/vulnerability-tests/7"/></refs></nvt><scan_nvt_version>2023-06-22T10:34:15Z</scan_nvt_version><threat>Log
/qod><description>Nmap service detection (unknown) result for this port: pando-pub

This is a guess. A confident identification of the service was not possible.

Hint: If you&apos;re running a recent nmap version try to run nmap with the following command: &apos;nmap -sV -
int to the nmap database.
</description><original_threat>Log</original_threat><original_severity>0</original_severity><compliance>undefined
78"><name>Hostname Determination Reporting</name><owner><name>admin2</name></owner><modification_
08-07T13:26:41Z</creation_time><report id="d057bfbe-4ae6-4d2d-b173-b990da552a56"/><task id="17cb935e-cb10-
1<asset asset_id="459291f2-4d4d-4fc9-83e9-fb610ad0de35"/><hostname></hostname></host><port>general/tcp</
etermination Reporting</name><family>Service detection</family><cvss_base>0.0</cvss_base><severities score="0
3:26Z</date><score>0.0</score><value>AV:N/AC:L/Au:N/C:N/I:N/A:N</value></severity></severities><tags>cvss_bas
on on how the hostname of the target
  was determined.|insight=|affected=|impact=|solution=|vuldetect=|solution_type=</tags><solution type=''></solu
hreat>Log</threat><severity>0.0</severity><qod><value>80</value><type></type></qod><description>Hostname d

Hostname|Source
192.168.56.1|IP-address
</description><original_threat>Log</original_threat><original_severity>0</original_severity><compliance>undefined
36"><name>DCE/RPC and MSRPC Services Enumeration</name><owner><name>admin2</name></owner><modifi
>2025-08-07T13:18:40Z</creation_time><report id="d057bfbe-4ae6-4d2d-b173-b990da552a56"/><task id="17cb935
68.56.1<asset asset_id="459291f2-4d4d-4fc9-83e9-fb610ad0de35"/><hostname></hostname></host><port>135/tcp
and MSRPC Services Enumeration</name><family>Service detection</family><cvss_base>0.0</cvss_base><severitie
-03T13:08:04Z</date><score>0.0</score><value>AV:N/AC:L/Au:N/C:N/I:N/A:N</value></severity></severities><tags>
g Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running
  on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

  The actual reporting takes place in the VT &apos;DCE/RPC and MSRPC Services Enumeration Reporting&apos;
  (OID: 1.3.6.1.4.1.25623.1.0.10736)|insight=|affected=|impact=An attacker may use this fact to gain more knowledg
  about the remote host.|solution=Filter incoming traffic to this port.|vuldetect=|solution_type=Mitigation</tags><so
solution></nvt><scan_nvt_version>2023-06-22T10:34:15Z</scan_nvt_version><threat>Log</threat><severity>0.0</se
int resolution service seems to be running on this port.
</description><original_threat>Log</original_threat><original_severity>0</original_severity><compliance>undefined
=70 sort-reverse=severity rows=10 first=1</term><keywords><keyword><column>apply_overrides</column><relatio
relation>=</relation><value>70</value></keyword><keyword><column>sort-reverse</column><relation>=</relation
=</relation><value>10</value></keyword><keyword><column>first</column><relation>=</relation><value>1</valu
der></field></sort><results start="1" max="10"/><result_count>13<filtered>11</filtered><page>10</page></result_
```