Scan Report

May 25, 2021

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "windows_highest_Port setting". The scan started at Thu May 20 08:57:03 2021 UTC and ended at Thu May 20 09:08:32 2021 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.178.49 sn-desktop.fritz.box	0	1	0	27	0
Total: 1	0	1	0	27	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "High" are not shown.
Issues with the threat level "Medium" are not shown.
Issues with the threat level "Low" are not shown.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 28 results selected by the filtering described above. Before filtering there were 30 results.

2 Results per Host

2.1 192.168.178.49

Host scan start	Thu May 20 08:57:25 2021 UTC
Host scan end	Thu May 20 09:08:28 2021 UTC

Service (Port)	Threat Level
135/tcp	Medium
49665/tcp	Log
general/CPE-T	Log
135/tcp	Log
7680/tcp	Log
3306/tcp	Log
49667/tcp	Log
49713/tcp	Log
17500/tcp	Log
49772/tcp	Log
33060/tcp	Log
5357/tcp	Log

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
49676/tcp	Log
49671/tcp	Log
54785/tcp	Log
139/tcp	Log
general/tcp	Log
57995/tcp	Log
49664/tcp	Log
49666/tcp	Log
445/tcp	Log

2.1.1 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing 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.

Vulnerability Detection Result
```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.178.49[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:192.168.178.49[49664]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.178.49[49664]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.178.49[49664]
     Annotation: KeyIso
Port: 49665/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.178.49[49665]
Port: 49666/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.178.49[49666]
     Annotation: Event log TCPIP
```

... continues on next page ...

... continued from previous page ...

```
Port: 49667/tcp
      UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
      Endpoint: ncacn_ip_tcp:192.168.178.49[49667]
      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:192.168.178.49[49667]
Port: 49671/tcp
      UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
      Endpoint: ncacn_ip_tcp:192.168.178.49[49671]
Port: 49676/tcp
      UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
      Endpoint: ncacn_ip_tcp:192.168.178.49[49676]
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.178.49[49676]
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
      Endpoint: ncacn_ip_tcp:192.168.178.49[49676]
      UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
      Endpoint: ncacn_ip_tcp:192.168.178.49[49676]
      UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
      Endpoint: ncacn_ip_tcp:192.168.178.49[49676]
Port: 49713/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:192.168.178.49[49713]
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: 2017-06-13T07:06:12Z

[return to 192.168.178.49]

2.1.2 Log 49665/tcp

Log (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing 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.

Vulnerability Detection Result
```
The following DCE/RPC or MSRPC services are running on this port:
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.178.49[49665]
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: `DCE/RPC and MSRPC Services Enumeration Reporting`
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: `2017-06-13T07:06:12Z`

[return to 192.168.178.49]

2.1.3 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.
Note: Some CPEs for specific products might show up twice or more in the output. Background: After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.

Vulnerability Detection Result
`192.168.178.49|cpe:/o:microsoft:windows`

Solution:

. . . continues on next page . . .

... continued from previous page ...

Log Method
Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `2021-04-16T10:39:13Z`

References
`url: https://nvd.nist.gov/products/cpe`

[return to 192.168.178.49]

2.1.4 Log 135/tcp

Log (CVSS: 0.0)
NVT: DCE/RPC and MSRPC Services Enumeration

Summary
Distributed Computing 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 NVT 'DCE/RPC and MSRPC Services Enumeration Reporting' (OID: 1.3.6.1.4.1.25623.1.0.10736)

Vulnerability Detection Result
`A DCE endpoint resolution service seems to be running on this port.`

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this port.

Log Method
Details: `DCE/RPC and MSRPC Services Enumeration`
OID:1.3.6.1.4.1.25623.1.0.108044
Version used: `2021-04-15T13:23:31Z`

[return to 192.168.178.49]

2.1.5 Log 7680/tcp

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This NVT consolidates and reports the information collected by the following NVTs:
- 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 portal.

Vulnerability Detection Result
```
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're running a recent nmap version try to run nmap with the following
↪ command: 'nmap -sV -Pn -p 7680 192.168.178.49' and submit a possible collecte
↪d fingerprint to the nmap database.
```

Solution:

Log Method
Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `2019-01-03T20:41:17Z`

References
`url: https://community.greenbone.net/c/vulnerability-tests`

[return to 192.168.178.49]

2.1.6 Log 3306/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A MySQL server is running on this port`

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2021-03-15T10:42:03Z`

[return to 192.168.178.49]

2.1.7 Log 49667/tcp

Log (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing 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.

Vulnerability Detection Result
```
The following DCE/RPC or MSRPC services are running on this port:
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.178.49[49667]
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.178.49[49667]
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: `DCE/RPC and MSRPC Services Enumeration Reporting`
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: `2017-06-13T07:06:12Z`

[return to 192.168.178.49]

2.1.8 Log 49713/tcp

Log (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing 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.

Vulnerability Detection Result
```
The following DCE/RPC or MSRPC services are running on this port:
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.178.49[49713]
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: `DCE/RPC and MSRPC Services Enumeration Reporting`
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: `2017-06-13T07:06:12Z`

[return to 192.168.178.49]

2.1.9 Log 17500/tcp

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This NVT consolidates and reports the information collected by the following NVTs:
- 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 portal.

Vulnerability Detection Result
```
Nmap service detection (unknown) result for this port: ssl|db-lsp
This is a guess. A confident identification of the service was not possible.
Hint: If you're running a recent nmap version try to run nmap with the following
↪ command: 'nmap -sV -Pn -p 17500 192.168.178.49' and submit a possible collect
```

... continues on next page ...

... continued from previous page ...

↪ed fingerprint to the nmap database.

Solution:

Log Method
Details: Unknown OS and Service Banner Reporting
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: 2019-01-03T20:41:17Z

References
url: https://community.greenbone.net/c/vulnerability-tests

[return to 192.168.178.49]

2.1.10 Log 49772/tcp

Log (CVSS: 0.0)
NVT: Check open ports

Summary
This plugin checks if the port scanners did not kill a service.

Vulnerability Detection Result
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by a plugin

Solution:

Log Method
Details: Check open ports
OID:1.3.6.1.4.1.25623.1.0.10919
Version used: 2019-02-20T11:12:24Z

[return to 192.168.178.49]

2.1.11 Log 33060/tcp

Log (CVSS: 0.0)
NVT: Services

Summary

... continues on next page ...

... continued from previous page ...

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A SOCKS5 proxy is running on this port.`

Solution:

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2021-03-15T10:42:03Z`

[return to 192.168.178.49]

2.1.12 Log 5357/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A web server is running on this port`

Solution:

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2021-03-15T10:42:03Z`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
The remote HTTP Server banner is:
Server: Microsoft-HTTPAPI/2.0

Solution:

Log Method
Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2020-08-24T15:18:35Z

Log (CVSS: 0.0)
NVT: HTTP Server Banner Enumeration

Summary
This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

Vulnerability Detection Result
It was possible to enumerate the following HTTP server banner(s):

Server banner	Enumeration technique
Server: Microsoft-HTTPAPI/2.0	Valid HTTP 0.9 GET request to '/index.html'

Solution:

Log Method
Details: HTTP Server Banner Enumeration
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: 2021-01-11T11:29:35Z

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use

... continues on next page ...

... continued from previous page ...

- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result

```
The Hostname/IP "sn-desktop.fritz.box" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
This service seems to be able to host PHP scripts.
This service seems to be able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 20.8.1)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://sn-desktop.fritz.box:5357/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method

Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2020-11-19T14:17:11Z

References

url: https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary

All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------
↪----------------------------------------------------------------------------
```

... continues on next page ...

... continued from previous page ...

```
↪--------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-01-26T13:20:44Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.io/

[return to 192.168.178.49]

2.1.13 Log 49676/tcp

Log (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing 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.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
The following DCE/RPC or MSRPC services are running on this port:
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:192.168.178.49[49676]
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:192.168.178.49[49676]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:192.168.178.49[49676]
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:192.168.178.49[49676]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:192.168.178.49[49676]
```

Impact

An attacker may use this fact to gain more knowledge about the remote host.

Solution:

Solution type: Mitigation

Filter incoming traffic to this ports.

Vulnerability Detection Method

Details: `DCE/RPC and MSRPC Services Enumeration Reporting`

OID:1.3.6.1.4.1.25623.1.0.10736

Version used: `2017-06-13T07:06:12Z`

[return to 192.168.178.49]

2.1.14 Log 49671/tcp

Log (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary

Distributed Computing 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.

Vulnerability Detection Result

```
The following DCE/RPC or MSRPC services are running on this port:
     UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
     Endpoint: ncacn_ip_tcp:192.168.178.49[49671]
```

... continues on next page ...

... continued from previous page ...

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: `DCE/RPC and MSRPC Services Enumeration Reporting`
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: `2017-06-13T07:06:12Z`

[return to 192.168.178.49]

2.1.15 Log 54785/tcp

Log (CVSS: 0.0)
NVT: Check open ports

Summary
This plugin checks if the port scanners did not kill a service.

Vulnerability Detection Result
```
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by a plugin
```

Solution:

Log Method
Details: `Check open ports`
OID:1.3.6.1.4.1.25623.1.0.10919
Version used: `2019-02-20T11:12:24Z`

[return to 192.168.178.49]

2.1.16 Log 139/tcp

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary

... continues on next page ...

... continued from previous page ...

This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Vulnerability Detection Result
`A SMB server is running on this port`

Solution:

Log Method
Details: `SMB/CIFS Server Detection`
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: `2020-11-10T15:30:28Z`

[return to 192.168.178.49]

2.1.17 Log general/tcp

Log (CVSS: 0.0)
NVT: Traceroute

Summary
Collect information about the network route and network distance between the scanner host and the target host.

Vulnerability Detection Result
```
Network route from scanner (10.0.2.15) to target (192.168.178.49):
10.0.2.15
192.168.178.49
Network distance between scanner and target: 2
```

Solution:

Vulnerability Insight
For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.

Log Method
A combination of the protocols ICMP and TCP is used to determine the route. This method is applicable for IPv4 only and it is also known as 'traceroute'.
Details: `Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `2021-03-12T14:25:59Z`

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script 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 portal.

Vulnerability Detection Result

```
Best matching OS:
OS:           Microsoft Windows
CPE:          cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (Operating System (OS) Detection (HTT
↪P))
Concluded from HTTP Server banner on port 5357/tcp: Server: Microsoft-HTTPAPI/2.
↪0
Setting key "Host/runs_windows" based on this information
Other OS detections (in order of reliability):
OS:           Microsoft Windows
CPE:          cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.108044 (DCE/RPC and MSRPC Services Enumerati
↪on)
Concluded from DCE/RPC and MSRPC Services Enumeration on port 135/tcp
```

Solution:

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2021-05-17T10:34:03Z

References
url: https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: Hostname Determination Reporting

Summary
The script reports information on how the hostname of the target was determined.

Vulnerability Detection Result

```
Hostname determination for IP 192.168.178.49:
Hostname|Source
```

. . . continues on next page . . .

... continued from previous page ...

sn-desktop.fritz.box | Reverse-DNS
Solution:
Log Method Details: Hostname Determination Reporting OID:1.3.6.1.4.1.25623.1.0.108449 Version used: 2018-11-19T11:11:31Z

[return to 192.168.178.49]

2.1.18 Log 57995/tcp

Log (CVSS: 0.0) NVT: Check open ports
Summary This plugin checks if the port scanners did not kill a service.
Vulnerability Detection Result This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by a plugin
Solution:
Log Method Details: Check open ports OID:1.3.6.1.4.1.25623.1.0.10919 Version used: 2019-02-20T11:12:24Z

[return to 192.168.178.49]

2.1.19 Log 49664/tcp

Log (CVSS: 5.0) NVT: DCE/RPC and MSRPC Services Enumeration Reporting
Summary Distributed Computing 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.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
The following DCE/RPC or MSRPC services are running on this port:
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.178.49[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:192.168.178.49[49664]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.178.49[49664]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.178.49[49664]
     Annotation: KeyIso
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: `DCE/RPC and MSRPC Services Enumeration Reporting`
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: `2017-06-13T07:06:12Z`

[return to 192.168.178.49]

2.1.20 Log 49666/tcp

Log (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing 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.

Vulnerability Detection Result

```
The following DCE/RPC or MSRPC services are running on this port:
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.178.49[49666]
```

... continues on next page ...

... continued from previous page ...

Annotation: Event log TCPIP

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: 2017-06-13T07:06:12Z

[return to 192.168.178.49]

2.1.21 Log 445/tcp

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary
This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Vulnerability Detection Result
A CIFS server is running on this port

Solution:

Log Method
Details: SMB/CIFS Server Detection
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: 2020-11-10T15:30:28Z

Log (CVSS: 0.0)
NVT: SMB Remote Version Detection

Summary
Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Only SMBv2 is enabled on remote target

Solution:

Log Method
Details: SMB Remote Version Detection
OID:1.3.6.1.4.1.25623.1.0.807830
Version used: 2019-05-16T07:13:31Z

[return to 192.168.178.49]