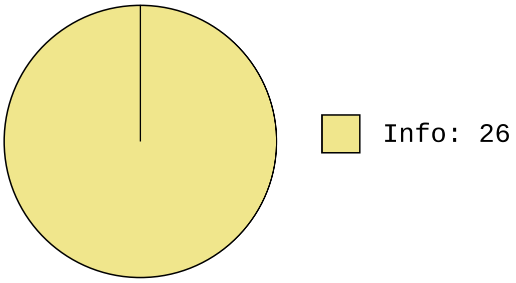
AlienVault: I.T Security Vulnerability Report

Scan time:	-	Generated:	2024-05-01 16:07:01

Total number of vulnerabilities identified on 4 system(s)



Total number of vulnerabilities identified per system

HostIP	HostName	Critical	High	Med	Low	Info
10.147.17.206	ProductionLayer3	--	--	--	--	6
10.147.17.233	JuansProduction	--	--	--	--	11
10.147.17.79	OssimSensor0	--	--	--	--	2
10.147.17.90	Host-10-147-17-90	--	--	--	--	7

10.147.17.79	OssimSensor0

Info:

OS Detection Consolidation and Reporting
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 105937
Vulnerability Detection Result:
Best matching OS:
OS: Linux Kernel
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (Operating System (OS) Detection (ICMP))
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
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.
References:
URL:https://community.greenbone.net/c/vulnerability-tests
CVSS Base Score:
0.0
Family name: Product detection
Category: infos
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.
Created: 2016-02-19T10:19:54Z
Modified: 2022-04-05T09:27:51Z

Info:

Traceroute

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 51662

Vulnerability Detection Result:

Network route from scanner (10.147.17.76) to target (10.147.17.79):
10.147.17.76
10.147.17.79

Network distance between scanner and target: 2

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

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

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.

Vulnerability Detection 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'.

CVSS Base Score:

0.0

Family name: General

Category: infos

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

Created: 2010-07-08T17:27:45Z

Modified: 2021-03-12T14:25:59Z

10.147.17.90	Host-10-147-17-90
Info: Services Risk: Info Application: unknown Port: 25672 Protocol: tcp ScriptID: 10330 Vulnerability Detection Result: The service closed the connection after 7 seconds without sending any data It might be protected by some TCP wrapper CVSS Base Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N 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. CVSS Base Score: 0.0 Family name: Service detection Category: infos 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. Created: 2011-01-14T09:12:23Z Modified: 2021-03-15T10:42:03Z	

```
Info:

    Hostname Determination Reporting
    Risk: Info
    Application: general
    Port: 0
    Protocol: tcp
    ScriptID: 108449
    Vulnerability Detection Result:
    Hostname determination for IP 10.147.17.90:
    Hostname|Source
    10.147.17.90|IP-address
    CVSS Base Vector:
    AV:N/AC:L/Au:N/C:N/I:N/A:N
    Summary:
    The script reports information on how the hostname
      of the target was determined.
    CVSS Base Score:
    0.0
    Family name: Service detection
    Category: end
    Summary: The script reports information on how the hostname
      of the target was determined.
    Created: 2018-07-05T06:03:26Z
    Modified: 2018-11-19T11:11:31Z
```

Info:

Services

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A web server is running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

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.

CVSS Base Score:

0.0

Family name: Service detection

Category: infos

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.

Created: 2011-01-14T09:12:23Z

Modified: 2021-03-15T10:42:03Z

Info:

Services

Risk: Info

Application: http-alt

Port: 8000

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A web server is running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

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.

CVSS Base Score:

0.0

Family name: Service detection

Category: infos

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.

Created: 2011-01-14T09:12:23Z

Modified: 2021-03-15T10:42:03Z

Info:

Services

Risk: Info

Application: unknown

Port: 9993

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A web server is running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

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.

CVSS Base Score:

0.0

Family name: Service detection

Category: infos

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.

Created: 2011-01-14T09:12:23Z

Modified: 2021-03-15T10:42:03Z

Info:

Services

Risk: Info

Application: unknown

Port: 5601

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A web server is running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

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.

CVSS Base Score:

0.0

Family name: Service detection

Category: infos

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.

Created: 2011-01-14T09:12:23Z

Modified: 2021-03-15T10:42:03Z

Info:

Services

Risk: Info

Application: unknown

Port: 15672

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A web server is running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

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.

CVSS Base Score:

0.0

Family name: Service detection

Category: infos

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.

Created: 2011-01-14T09:12:23Z

Modified: 2021-03-15T10:42:03Z

10.147.17.206	ProductionLayer3
Info: Hostname Determination Reporting Risk: Info Application: general Port: 0 Protocol: tcp ScriptID: 108449 Vulnerability Detection Result: Hostname determination for IP 10.147.17.206: Hostname|Source 10.147.17.206|IP-address CVSS Base Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N Summary: The script reports information on how the hostname of the target was determined. CVSS Base Score: 0.0 Family name: Service detection Category: end Summary: The script reports information on how the hostname of the target was determined. Created: 2018-07-05T06:03:26Z Modified: 2018-11-19T11:11:31Z	

Info:

Services
Risk: Info
Application: unknown
Port: 15672
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A web server is running on this port
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
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.
CVSS Base Score:
0.0
Family name: Service detection
Category: infos
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.
Created: 2011-01-14T09:12:23Z
Modified: 2021-03-15T10:42:03Z

Info:

Services

Risk: Info

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

An ssh server is running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

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.

CVSS Base Score:

0.0

Family name: Service detection

Category: infos

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.

Created: 2011-01-14T09:12:23Z

Modified: 2021-03-15T10:42:03Z

Info:

Services

Risk: Info

Application: http-alt

Port: 8000

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A web server is running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

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.

CVSS Base Score:

0.0

Family name: Service detection

Category: infos

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.

Created: 2011-01-14T09:12:23Z

Modified: 2021-03-15T10:42:03Z

Info:

Services
Risk: Info
Application: mysql
Port: 3306
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
An unknown service is running on this port.
It is usually reserved for MySQL
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
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.
CVSS Base Score:
0.0
Family name: Service detection
Category: infos
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.
Created: 2011-01-14T09:12:23Z
Modified: 2021-03-15T10:42:03Z

```
Info:

    MariaDB / Oracle MySQL Detection (MySQL Protocol)
    Risk: Info
    Application: mysql
    Port: 3306
    Protocol: tcp
    ScriptID: 100152
    Vulnerability Detection Result:
    Detected Oracle MySQL
    Version:      8.0.36-0ubuntu0.22.04.1
    Location:     3306/tcp
    CPE:          cpe:/a:oracle:mysql:8.0.36
    Concluded from version/product identification result:
    8.0.36-0ubuntu0.22.04.1
    CVSS Base Vector:
    AV:N/AC:L/Au:N/C:N/I:N/A:N
    Summary:
    MySQL protocol-based detection of MariaDB / Oracle MySQL.
    CVSS Base Score:
    0.0
    Family name: Product detection
    Category: infos
    Summary: MySQL protocol-based detection of MariaDB / Oracle MySQL.
    Created: 2009-04-23T19:21:19Z
    Modified: 2021-02-12T06:42:15Z
```

10.147.17.233	JuansProduction
Info: Hostname Determination Reporting Risk: Info Application: general Port: 0 Protocol: tcp ScriptID: 108449 Vulnerability Detection Result: Hostname determination for IP 10.147.17.233: Hostname|Source 10.147.17.233|IP-address CVSS Base Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N Summary: The script reports information on how the hostname of the target was determined. CVSS Base Score: 0.0 Family name: Service detection Category: end Summary: The script reports information on how the hostname of the target was determined. Created: 2018-07-05T06:03:26Z Modified: 2018-11-19T11:11:31Z	

Info:

Services
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A TLScustom server answered on this port
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
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.
CVSS Base Score:
0.0
Family name: Service detection
Category: infos
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.
Created: 2011-01-14T09:12:23Z
Modified: 2021-03-15T10:42:03Z

Info:

Services

Risk: Info

Application: http-alt

Port: 8000

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A TLScustom server answered on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

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.

CVSS Base Score:

0.0

Family name: Service detection

Category: infos

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.

Created: 2011-01-14T09:12:23Z

Modified: 2021-03-15T10:42:03Z

Info:

Services

Risk: Info

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

An ssh server is running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

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.

CVSS Base Score:

0.0

Family name: Service detection

Category: infos

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.

Created: 2011-01-14T09:12:23Z

Modified: 2021-03-15T10:42:03Z

Info:

Services

Risk: Info

Application: mysql

Port: 3306

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

An unknown service is running on this port.

It is usually reserved for MySQL

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

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.

CVSS Base Score:

0.0

Family name: Service detection

Category: infos

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.

Created: 2011-01-14T09:12:23Z

Modified: 2021-03-15T10:42:03Z

Info:

Services
Risk: Info
Application: unknown
Port: 15672
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A web server is running on this port
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
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.
CVSS Base Score:
0.0
Family name: Service detection
Category: infos
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.
Created: 2011-01-14T09:12:23Z
Modified: 2021-03-15T10:42:03Z

Info:

SSL/TLS: Version Detection
Risk: Info
Application: http-alt
Port: 8000
Protocol: tcp
ScriptID: 105782
Vulnerability Detection Result:
The remote SSL/TLS service supports the following SSL/TLS protocol version(s):
TLSv1.2
TLSv1.3
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
Enumeration and reporting of SSL/TLS protocol versions supported
by a remote service.
Vulnerability Detection Method:
Sends multiple connection requests to the remote service and
attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported
independently from the allowed / supported SSL/TLS ciphers.
CVSS Base Score:
0.0
Family name: SSL and TLS
Category: infos
Summary: Enumeration and reporting of SSL/TLS protocol versions supported
by a remote service.
Created: 2016-06-29T08:54:20Z
Modified: 2021-12-06T15:42:24Z

```
Info:

    SSL/TLS: Version Detection
    Risk: Info
    Application: https
    Port: 443
    Protocol: tcp
    ScriptID: 105782
    Vulnerability Detection Result:
    The remote SSL/TLS service supports the following SSL/TLS protocol version(s):
    TLSv1.2
    TLSv1.3
    CVSS Base Vector:
    AV:N/AC:L/Au:N/C:N/I:N/A:N
    Summary:
    Enumeration and reporting of SSL/TLS protocol versions supported
      by a remote service.
    Vulnerability Detection Method:
    Sends multiple connection requests to the remote service and
      attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
      Note: The supported SSL/TLS protocol versions included in the report of this VT are reported
      independently from the allowed / supported SSL/TLS ciphers.
    CVSS Base Score:
    0.0
    Family name: SSL and TLS
    Category: infos
    Summary: Enumeration and reporting of SSL/TLS protocol versions supported
      by a remote service.
    Created: 2016-06-29T08:54:20Z
    Modified: 2021-12-06T15:42:24Z
```

```
Info:

    MariaDB / Oracle MySQL Detection (MySQL Protocol)
    Risk: Info
    Application: mysql
    Port: 3306
    Protocol: tcp
    ScriptID: 100152
    Vulnerability Detection Result:
    Detected Oracle MySQL
    Version:       8.0.36-0ubuntu0.22.04.1
    Location:      3306/tcp
    CPE:           cpe:/a:oracle:mysql:8.0.36
    Concluded from version/product identification result:
    8.0.36-0ubuntu0.22.04.1
    CVSS Base Vector:
    AV:N/AC:L/Au:N/C:N/I:N/A:N
    Summary:
    MySQL protocol-based detection of MariaDB / Oracle MySQL.
    CVSS Base Score:
    0.0
    Family name: Product detection
    Category: infos
    Summary: MySQL protocol-based detection of MariaDB / Oracle MySQL.
    Created: 2009-04-23T19:21:19Z
    Modified: 2021-02-12T06:42:15Z
```

Info:

Services

Risk: Info

Application: https

Port: 443

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A web server is running on this port through SSL

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

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.

CVSS Base Score:

0.0

Family name: Service detection

Category: infos

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.

Created: 2011-01-14T09:12:23Z

Modified: 2021-03-15T10:42:03Z

Info:

Services
Risk: Info
Application: http-alt
Port: 8000
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A web server is running on this port through SSL
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
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.
CVSS Base Score:
0.0
Family name: Service detection
Category: infos
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.
Created: 2011-01-14T09:12:23Z
Modified: 2021-03-15T10:42:03Z