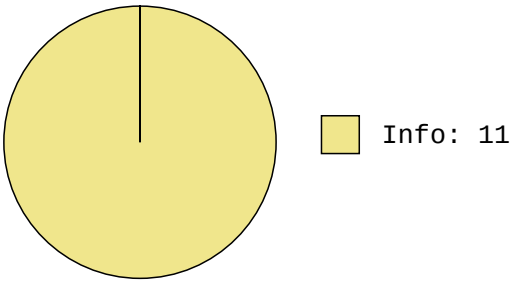
AlienVault: I.T Security Vulnerability Report

Job Name:	Extra Credit Scan	Scan time:	2024-04-30 14:39:52
Profile:	Base - Basic configuration template with a minimum set o...	Generated:	2024-04-30 17:12:44

Total number of vulnerabilities identified on 1 system(s)



Total number of vulnerabilities identified per system

HostIP	HostName	Critical	High	Med	Low	Info
10.147.17.233	Host-10-147-17-233	--	--	--	--	11

10.147.17.233	Host-10-147-17-233

Hostname Determination Reporting

Risk: Info
Application: general
Port: 0
Protocol: tcp
Script ID: 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

Created:
2018-07-05T06:03:26Z

Modified:
2018-11-19T11:11:31Z

MariaDB / Oracle MySQL Detection (MySQL Protocol)

Risk: Info
Application: mysql
Port: 3306
Protocol: tcp
Script ID: 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

Created:
2009-04-23T19:21:19Z

Modified:
2021-02-12T06:42:15Z

SSL/TLS: Version Detection

Risk: Info
Application: https
Port: 443
Protocol: tcp
Script ID: 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

Created:
2016-06-29T08:54:20Z

Modified:
2021-12-06T15:42:24Z

Services

Risk: Info
Application: mysql
Port: 3306
Protocol: tcp
Script ID: 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

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

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

Services

Risk: Info
Application: https
Port: 443
Protocol: tcp
Script ID: 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

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

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

Services

Risk: Info
Application: https
Port: 443
Protocol: tcp
Script ID: 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

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

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

Services

Risk: Info
Application: unknown
Port: 15672
Protocol: tcp
Script ID: 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

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

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

Services

Risk: Info
Application: http-alt
Port: 8000
Protocol: tcp
Script ID: 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

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

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

Services

Risk: Info
Application: ssh
Port: 22
Protocol: tcp
Script ID: 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

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

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

Services

Risk: Info
Application: http-alt
Port: 8000
Protocol: tcp
Script ID: 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

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

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

SSL/TLS: Version Detection

Risk: Info
Application: http-alt
Port: 8000
Protocol: tcp
Script ID: 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

Created:
2016-06-29T08:54:20Z

Modified:
2021-12-06T15:42:24Z