



NSD Dynamic Adv Scan

Report generated by Nessus™

Sat, 10 Jul 2021 02:58:36 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

• 184.73.185.129.....	4
-----------------------	---

Nessus Essentials

Vulnerabilities by Host

184.73.185.129



Scan Information

Start time: Sat Jul 10 02:41:30 2021
End time: Sat Jul 10 02:58:36 2021

Host Information

DNS Name: ec2-184-73-185-129.compute-1.amazonaws.com
IP: 184.73.185.129
OS: AIX 5.3

Vulnerabilities

10756 - Apple Mac OS X Find-By-Content .DS_Store Web Directory Listing

Synopsis

It is possible to get the list of files present in the remote directory.

Description

It is possible to read a '.DS_Store' file on the remote web server.

This file is created by MacOS X Finder; it is used to remember the icons position on the desktop, among other things, and contains the list of files and directories present in the remote directory.

Note that deleted files may still be present in this .DS_Store file.

See Also

<https://support.apple.com/en-us/HT1629>
<https://helpx.adobe.com/dreamweaver/kb/remove-ds-store-files-mac.html>
<http://www.greci.cc/?p=10>

Solution

- Configure your web server so as to prevent the download of .DS_Store files

- Mac OS X users should configure their workstation to disable the creation of .DS_Store files on network shares.

Risk Factor

Medium

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	3316
BID	3325
CVE	CVE-2001-1446
XREF	CERT:177243

Plugin Information

Published: 2001/09/14, Modified: 2018/11/15

Plugin Output

tcp/80/www

```
http://ec2-184-73-185-129.compute-1.amazonaws.com/.DS_Store
reveals the following entries:
assets
```

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	32319
CVE	CVE-2008-5161
XREF	CERT:958563
XREF	CWE:200

Plugin Information

Published: 2013/10/28, Modified: 2018/07/30

Plugin Output

tcp/22/ssh

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :
```

```
3des-cbc  
aes128-cbc  
aes192-cbc  
aes256-cbc  
blowfish-cbc  
cast128-cbc
```

The following server-to-client Cipher Block Chaining (CBC) algorithms are supported :

```
3des-cbc  
aes128-cbc  
aes192-cbc  
aes256-cbc  
blowfish-cbc  
cast128-cbc
```

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

<https://httpd.apache.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2020/09/22

Plugin Output

tcp/80/www

```
URL      : http://ec2-184-73-185-129.compute-1.amazonaws.com/
Version  : unknown
backported : 0
```


39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Give Nessus credentials to perform local checks.
```

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

<http://cpe.mitre.org/>

<https://nvd.nist.gov/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2021/06/03

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :
```

```
cpe:/o:ibm:aix:5.3 -> IBM AIX 5.3
```

```
Following application CPE's matched on the remote system :
```

```
cpe:/a:apache:http_server:
```

```
cpe:/a:openbsd:openssh:7.4 -> OpenBSD OpenSSH 7.4
```

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 65
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :  
Apache
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
184.73.185.129 resolves as ec2-184-73-185-129.compute-1.amazonaws.com.
```

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK
```

```
Protocol version : HTTP/1.1
```

```
SSL : no
```

```
Keep-Alive : yes
```

```
Options allowed : (Not implemented)
```

```
Headers :
```

```
    Date: Sat, 10 Jul 2021 06:56:40 GMT
```

```
    Server: Apache
```

```
    Cache-Control: no-cache
```

```
    Keep-Alive: timeout=65, max=100
```

```
    Connection: Keep-Alive
```

```
    Transfer-Encoding: chunked
```

```
    Content-Type: text/html; charset=UTF-8
```

```
Response Body :
```

```
<!DOCTYPE html>
```

```
<html lang="en">
```

```
  <head>
```

```
    <meta charset="utf-8">
```

```
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
```

```
    <title>Your Thoughts</title>
```

```
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
```

```

<link href="assets/css/bootstrap.min.css" rel="stylesheet">
<style>
  body {background: url(assets/img/background.png) repeat;}
  .hero-unit {background-color: white;}
</style>
<link href="assets/css/bootstrap-responsive.min.css" rel="stylesheet">
<!--[if lt IE 9]><script src="http://html5shim.googlecode.com/svn/trunk/html5.js"></script><![endif]-->
</head>

<body>

  <div class="container">

    <h1>Your Thoughts</h1>

    <p><a href="/add" class="btn"><b class="icon-pencil"></b> Share Your Thought</a></p>

    <div class="hero-unit">
      <div class="row-fluid">
        <blockquote>
          <p>Tik Tok</p>
          <small>Doc</small>
        </blockquote>
        <hr>
        <blockquote>
          <p>Spiros server
</p>
          <small>Spiros server</small>
        </blockquote>
        <hr>
        <blockquote>
          <p>Anrich</p>
          <small>Anrich</small>
        </blockquote>
        <hr>
        <blockquote>
          <p>test</p>
          <small>test</small>
        </blockquote>
        <hr>
        <blockquote>
          <p>c:/Windows/system.ini</p>
          <small>ZAP</small>
        </blockquote>
        <hr>
        <blockquote>
          <p>../../../../../../../../../../../../.. [...]

```

117886 - Local Checks Not Enabled (info)

Synopsis

Local checks were not enabled.

Description

Nessus did not enable local checks on the remote host. This does not necessarily indicate a problem with the scan. Credentials may not have been provided, local checks may not be available for the target, the target may not have been identified, or another issue may have occurred that prevented local checks from being enabled. See plugin output for details.

This plugin reports informational findings related to local checks not being enabled. For failure information, see plugin 21745 :

'Authentication Failure - Local Checks Not Run'.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2020/09/22

Plugin Output

tcp/0

The following issues were reported :

```
- Plugin      : no_local_checks_credentials.nasl
  Plugin ID   : 110723
  Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
  Message     :
  Credentials were not provided for detected SSH service.
```


Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/04/20

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2021/06/28

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 8.15.0
Nessus build : 20271
Plugin feed version : 202107100130
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian6-x86-64
Scan type : Normal
Scan name : NSD Dynamic Adv Scan
```

Scan policy used : Advanced Scan
Scanner IP : 10.0.2.15

WARNING : No port scanner was enabled during the scan. This may lead to incomplete results.

Port range : default
Ping RTT : 55.023 ms
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2021/7/10 2:41 EDT
Scan duration : 1016 sec

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2021/05/12

Plugin Output

tcp/0

```
Remote operating system : AIX 5.3  
Confidence level : 65  
Method : SinFP
```

```
The remote host is running AIX 5.3
```

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :
```

```
The server supports the following options for kex_algorithms :
```

```
curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
```

```
The server supports the following options for server_host_key_algorithms :
```

```
ecdsa-sha2-nistp256
rsa-sha2-256
rsa-sha2-512
ssh-ed25519
ssh-rsa
```

```
The server supports the following options for encryption_algorithms_client_to_server :
```

```
3des-cbc
aes128-cbc
```

```
aes128-ctr
aes128-gcm@openssh.com
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
aes256-gcm@openssh.com
blowfish-cbc
cast128-cbc
chacha20-poly1305@openssh.com
```

The server supports the following options for `encryption_algorithms_server_to_client` :

```
3des-cbc
aes128-cbc
aes128-ctr
aes128-gcm@openssh.com
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
aes256-gcm@openssh.com
blowfish-cbc
cast128-cbc
chacha20-poly1305@openssh.com
```

The server supports the following options for `mac_algorithms_client_to_server` :

```
hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
```

The server supports the following options for `mac_algorithms_server_to_client` :

```
hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
```

The server supports the following options for `compression_algorithms_client_to_server` :

```
none
zlib@openssh.com
```

The server supports the following options for `compression_algorithms_server_to_ [...]`

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2021/01/19

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the  
SSH protocol :
```

- 1.99
- 2.0

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_7.4
SSH supported authentication : publickey
```

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/22/ssh

```
An SSH server is running on this port.
```

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.
- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2021/01/25

Plugin Output

tcp/0

```
SSH was detected on port 22 but no credentials were provided.  
SSH local checks were not enabled.
```

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.0.2.15 to 184.73.185.129 :  
10.0.2.15  
10.0.2.2  
184.73.185.129  
  
Hop Count: 2
```