Rapport de Vulnérabilités

Généré le : 17/05/2025 20:04:21

Résumé du scan

Cible: 192.168.217.140

Heure du scan: 2025-05-17 20:04:21

État de l'hôte: up

2
Critiques

0
Élevées

0
Moyennes

0
Faibles

4
Informatives

Vulnérabilités détectées

ftp-vsftpd-backdoor

Port 21 ftp

```
  VULNERABLE:
  vsFTPd version 2.3.4 backdoor
    State: VULNERABLE (Exploitable)
    IDs:  BID:48539  CVE:CVE-2011-2523
      vsFTPd version 2.3.4 backdoor, this was
reported on 2011-07-04.
    Disclosure date: 2011-07-03
    Exploit results:
      Shell command: id
      Results: uid=0(root) gid=0(root)
    References:
      https://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2011-2523
      https://www.securityfocus.com/bid/48539
      https://github.com/rapid7/metasploit-
framework/blob/master/modules/exploits/unix/ftp/
vsftpd_234_backdoor.rb
      http://scarybeastsecurity.blogspot.com/
2011/07/alert-vsftpd-download-backdoored.html
```

ssl-dh-params

Port 25 smtp

```
  VULNERABLE:
  Anonymous Diffie-Hellman Key Exchange MitM
Vulnerability
    State: VULNERABLE
      Transport Layer Security (TLS) services
that use anonymous
      Diffie-Hellman key exchange only provide
protection against passive
      eavesdropping, and are vulnerable to active
man-in-the-middle attacks
      which could completely compromise the
```

```
confidentiality and integrity
   of any data exchanged over the resulting
session.
  Check results:
   ANONYMOUS DH GROUP 1
      Cipher Suite:
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
      Modulus Type: Safe prime
      Modulus Source: Unknown/Custom-
generated
      Modulus Length: 512
      Generator Length: 8
      Public Key Length: 512
  References:
   https://www.ietf.org/rfc/rfc2246.txt

 Transport Layer Security (TLS) Protocol
DHE_EXPORT Ciphers Downgrade MitM (Logjam)
  State: VULNERABLE
  IDs:  BID:74733  CVE:CVE-2015-4000
   The Transport Layer Security (TLS) protocol
contains a flaw that is
   triggered when handling Diffie-Hellman key
exchanges defined with
   the DHE_EXPORT cipher. This may allow a
man-in-the-middle attacker
   to downgrade the security of a TLS session
to 512-bit export-grade
   cryptography, which is significantly
weaker, allowing the attacker
   to more easily break the encryption and
monitor or tamper with
   the encrypted stream.
  Disclosure date: 2015-5-19
  Check results:
   EXPORT-GRADE DH GROUP 1
      Cipher Suite:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
      Modulus Type: Safe prime
      Modulus Source: Unknown/Custom-
generated
      Modulus Length: 512
      Generator Length: 8
      Public Key Length: 512
```

```
    References:
      https://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2015-4000
      https://weakdh.org
      https://www.securityfocus.com/bid/74733

  Diffie-Hellman Key Exchange Insufficient Group
Strength
    State: VULNERABLE
      Transport Layer Security (TLS) services
that use Diffie-Hellman groups
      of insufficient strength, especially those
using one of a few commonly
      shared groups, may be susceptible to
passive eavesdropping attacks.
    Check results:
      WEAK DH GROUP 1
            Cipher Suite:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
            Modulus Type: Safe prime
            Modulus Source: postfix builtin
            Modulus Length: 1024
            Generator Length: 8
            Public Key Length: 1024
    References:
      https://weakdh.org
```

smtp-vuln-cve2010-4344

Port 25 smtp

```

  The SMTP server is not Exim: NOT VULNERABLE
```

ssl-poodle

Port 25 smtp

```

  VULNERABLE:
  SSL POODLE information leak
    State: VULNERABLE
    IDs:  BID:70574  CVE:CVE-2014-3566
          The SSL protocol 3.0, as used in
OpenSSL through 1.0.1i and other
          products, uses nondeterministic CBC
padding, which makes it easier
          for man-in-the-middle attackers to
obtain cleartext data via a
          padding-oracle attack, aka the "POODLE"
issue.
    Disclosure date: 2014-10-14
    Check results:
      TLS_RSA_WITH_AES_128_CBC_SHA
    References:
      https://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2014-3566
      https://www.openssl.org/~bodo/ssl-
poodle.pdf
      https://www.imperialviolet.org/2014/10/14/
poodle.html
      https://www.securityfocus.com/bid/70574
```

http-slowloris-check

Port 80 http

```

  VULNERABLE:
  Slowloris DOS attack
    State: LIKELY VULNERABLE
    IDs:  CVE:CVE-2007-6750
      Slowloris tries to keep many connections to
the target web server open and hold
      them open as long as possible.  It
accomplishes this by opening connections to
      the target web server and sending a partial
request. By doing so, it starves
      the http server's resources causing Denial
Of Service.

    Disclosure date: 2009-09-17
    References:
      https://cve.mitre.org/cgi-bin/cvename.cgi?
```

```
name=CVE-2007-6750
      http://ha.ckers.org/slowloris/
```

http-vuln-cve2017-1001000

Port 80 http

```
ERROR: Script execution failed (use -d to debug)
```

Rapport généré automatiquement par Toolbox Cyber - 17/05/2025 20:04:21