BenchMark M3.srl

# Initial Vulnerability Scan

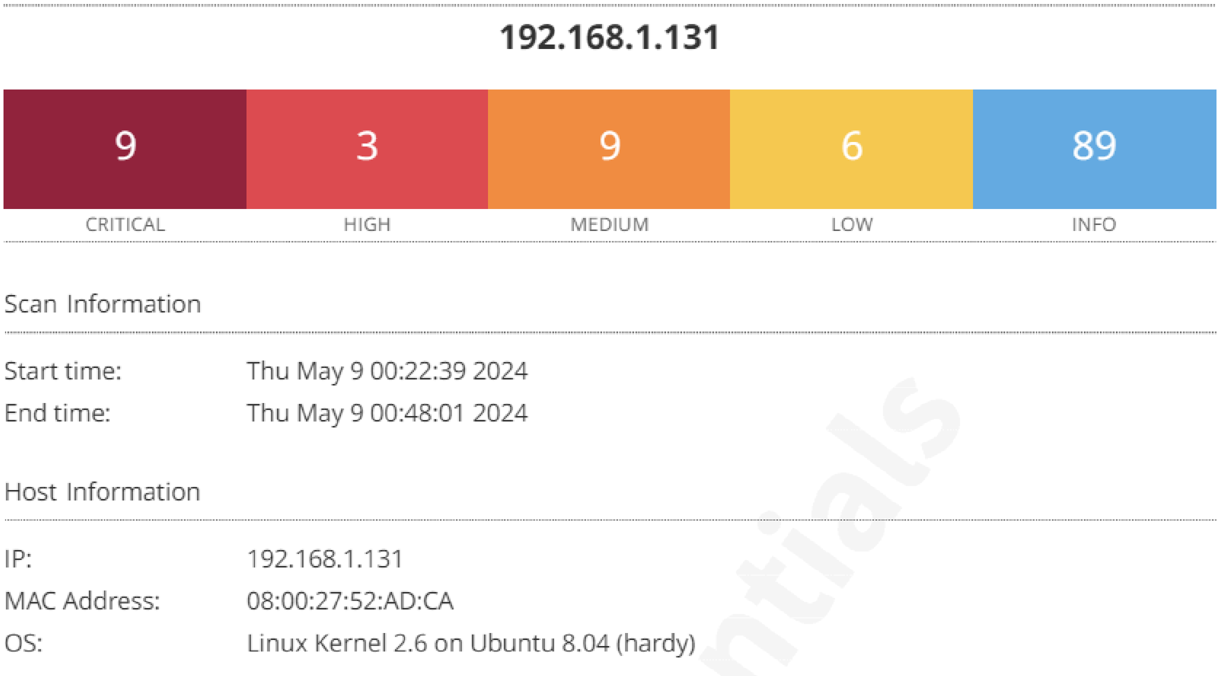
## Index

## Intro

In this presentation we will research the landscape of vulnerabilities present in the system, visually representing the entire spectrum of the threats.

This technical overview provides a clear insight into critical areas necessitating prompt interventions to ensure system security and integrity.

In the following we will show the chart with all vulnerabilities and next issues that we will address.



**192.168.1.131**

| CRITICAL | HIGH | MEDIUM | LOW | INFO |
|---|---|---|---|---|
| 9 | 3 | 9 | 6 | 89 |

Scan Information

| | |
|---|---|
| Start time: | Thu May 9 00:22:39 2024 |
| End time: | Thu May 9 00:48:01 2024 |

Host Information

| | |
|---|---|
| IP: | 192.168.1.131 |
| MAC Address: | 08:00:27:52:AD:CA |
| OS: | Linux Kernel 2.6 on Ubuntu 8.04 (hardy) |

## 51988 - Bind Shell Backdoor Detection

Synopsis: the remote host may have been compromised.

Description: a shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

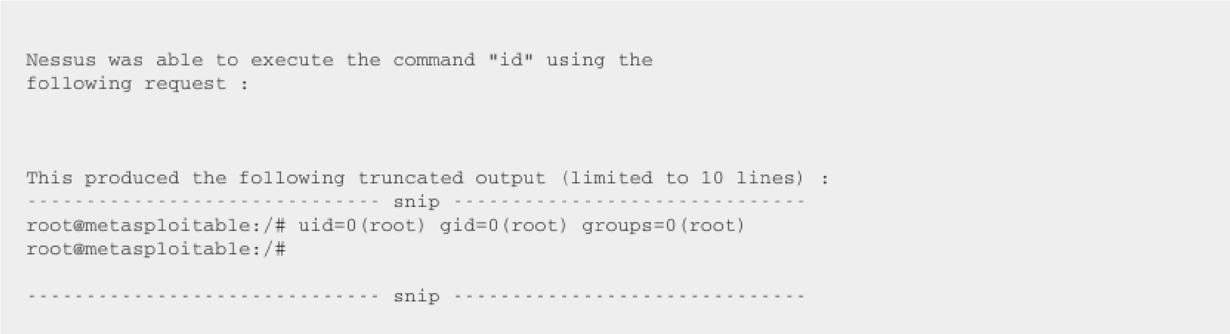
Risk Factor Critical

CVSS v3.0 Base Score 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information Published: 2011/02/15, Modified: 2022/04/11

Plugin Output tcp/1524/wild_shell



```
Nessus was able to execute the command "id" using the
following request :



This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

------------------------------ snip ------------------------------
```

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis: the remote SSH host keys are weak.

Description: the remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian package removing nearly all sources of entropy in the remote version of OpenSSL. An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

Risk Factor: Critical

VPR Score 5.1

CVSS v2.0 Base Score 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score 8.3 (CVSS2#E:F/RL:OF/RC:C)

References BID 29179 CVE CVE-2008-0166 XREF CWE:310

Exploitable With Core Impact (true)

Plugin Information Published: 2008/05/14, Modified: 2018/11/15

Plugin Output tcp/22/ssh

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Synopsis: the remote SSL certificate uses a weak key

Description: the remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian package removing nearly all sources of entropy in the remote version of OpenSSL. An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Solution Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor Critical

VPR Score 5.1

CVSS v2.0 Base Score 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score 8.3 (CVSS2#E:F/RL:OF/RC:C)

References BID 29179 CVE CVE-2008-0166 XREF CWE:310

Exploitable With Core Impact (true)

Plugin Information Published: 2008/05/15, Modified: 2020/11/16

Plugin Output tcp/5432/postgresql

## 20007 - SSL Version 2 and 3 Protocol Detection

Synopsis: the remote service encrypts traffic using a protocol with known weaknesses.

Description: the remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients. Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely. NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.

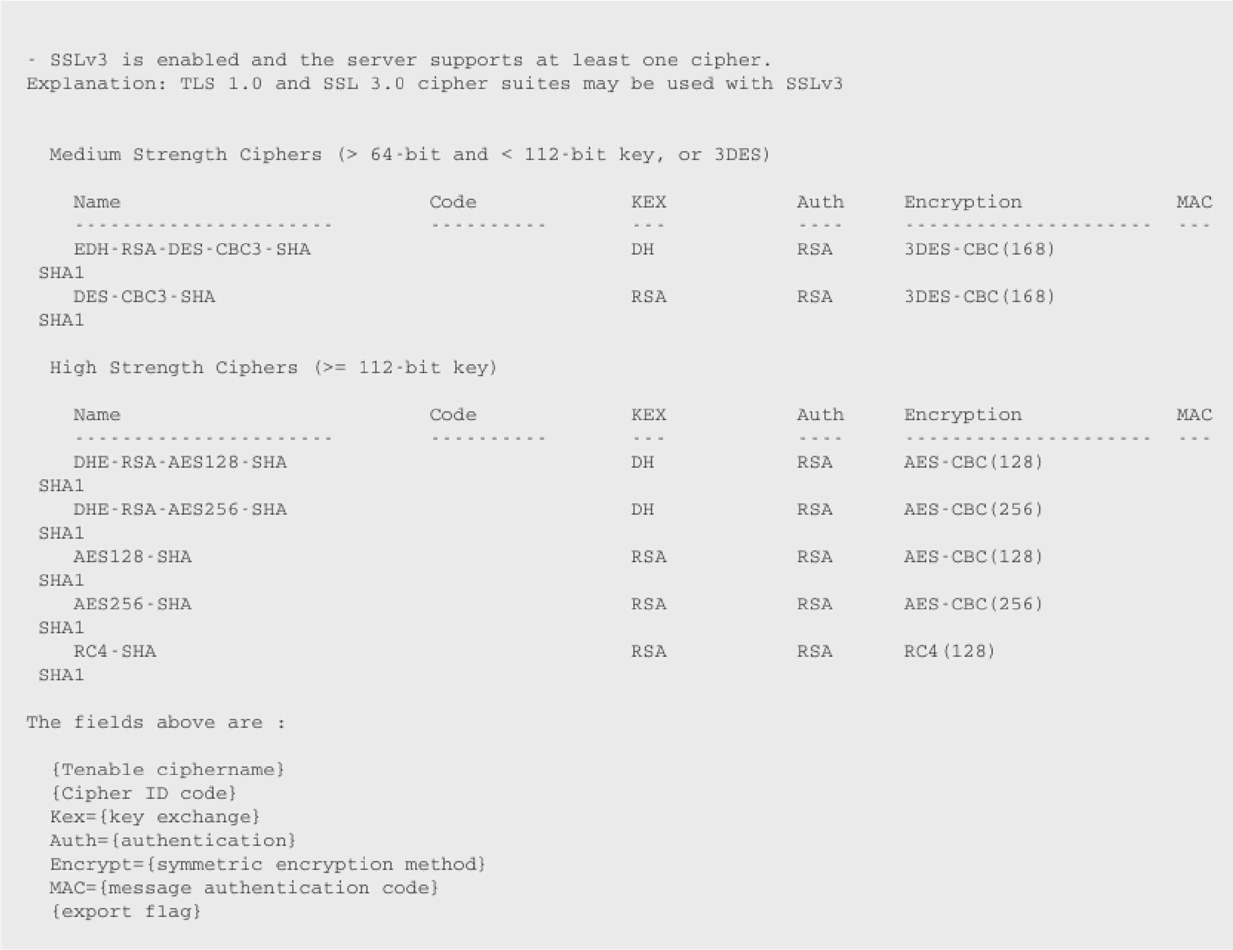
Risk Factor Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) CVSS v2.0 Base Score 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information Published: 2005/10/12, Modified: 2022/04/04

Plugin Output tcp/5432/postgresql



```
- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX        Auth     Encryption             MAC
    ----------------------        ----------       ---        ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA                           DH         RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                                   RSA        RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX        Auth     Encryption             MAC
    ----------------------        ----------       ---        ----     ---------------------  ---
    DHE-RSA-AES128-SHA                             DH         RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA                             DH         RSA      AES-CBC(256)
 SHA1
    AES128-SHA                                     RSA        RSA      AES-CBC(128)
 SHA1
    AES256-SHA                                     RSA        RSA      AES-CBC(256)
 SHA1
    RC4-SHA                                        RSA        RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 61708 - VNC Server 'password' Password

Synopsis: A VNC server running on the remote host is secured with a weak password

Description The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Risk Factor Critical

CVSS v2.0 Base Score 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information Published: 2012/08/29, Modified: 2015/09/24

Plugin Output tcp/5900/vnc