W12D4 - Analisi delle vulnerabilità e azioni di rimedio

INTRODUZIONE

Il presente report mostra i risultati di una scansione delle vulnerabilità effettuata sulla macchina target Metasploitable. L'obiettivo della scansione era identificare le vulnerabilità di sicurezza presenti nel sistema, così da valutarne il rischio complessivo e definire le azioni di rimedio appropriate.

La scansione è stata condotta utilizzando Tenable Nessus Essentials, e ha incluso una scansione completa delle porte TCP e UDP.

Per un elenco completo delle vulnerabilità rilevate e i dettagli tecnici completi, si veda **l'Appendice A: Report di Scansione Nessus.**

~~~

INFORMAZIONI DI BASE

- Data di inizio della scansione: Domenica 18 maggio 2025, 09:29
- Data di completamento della scansione: Domenica 18 maggio 2025, 09:39
- Macchina Target: METASPLOITABLE
- IP Macchina Target: 192.168.5.101
- OS Macchina Target: Linux Kernel 2.6 on Ubuntu 8.04
- Software utilizzato: Tenable Nessus Essentials

- Autore del report: **Pasquale Agizza**

~~~

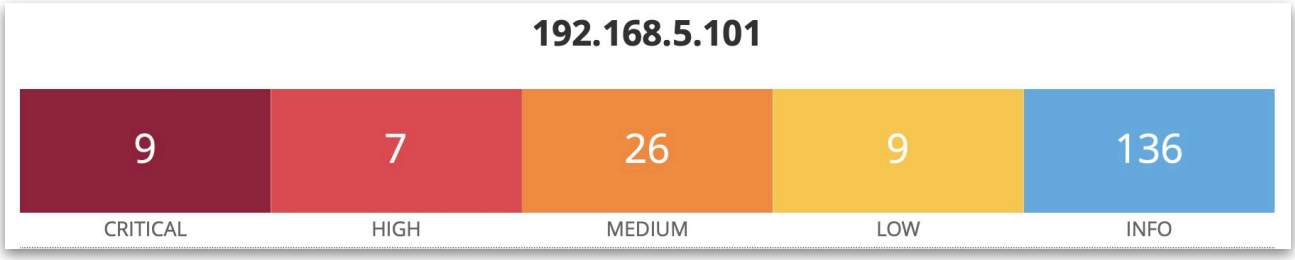
SOMMARIO

La scansione della macchina METASPLOITABLE ha rilevato **un totale di 187 vulnerabilità**, con rispettivamente 9 vulnerabilità Critical, 7 vulnerabilità High, 26 vulnerabilità Medium, 9 vulnerabilità Low e 136 vulnerabilità Info.

L'elevato numero di vulnerabilità, soprattutto quelle Critical, espone la macchina a un rischio di compromissione estremamente elevato.

A puro titolo esemplificativo, si possono citare la vulnerabilità "Canonical Ubuntu Linux SEoL (8.04.x)", che mette in mostra come il sistema operativo della macchina Target abbia ricevuto l'ultimo aggiornamento di sicurezza a maggio del 2013, o la vulnerabilità "VNC Server 'password' Password", che evidenzia come il server remoto VNC in esecuzione sulla macchina sia protetto da una password debole. Questo si traduce nella possibilità, per un attaccante, di prendere facilmente possesso della macchina.

La presenza e la gravità delle già citate vulnerabilità rende necessario intraprendere azioni immediate per la correzione delle stesse. Per ulteriori dettagli si veda **l'Appendice A: Report di Scansione Nessus.**



DESCRIZIONE DETTAGLIATA DELLE VULNERABILITÀ CRITICAL

In questa sezione allego la descrizione dettagliata delle 9 vulnerabilità critical evidenziate da Nessus:

• 134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

REFERENCE: CVE-2020-1745
CVE-2020-1938

- **SYNOPSIS**: There is a vulnerable AJP connector listening on the remote host.
- **DESCRIPTION**: A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE)
- **SOLUTION**: Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.
- **RISK FACTOR**: High
- **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)
- **PLUGIN OUTPUT**: tcp/8009/ajp13

• 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
- **SOLUTION**: Verify if the remote host has been compromised, and reinstall the system if necessary
- **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)
- **PLUGIN OUTPUT**: tcp/1524/wild_shell

• 201352 - Canonical Ubuntu Linux SEoL (8.04.x)

- **SYNOPSIS**: An unsupported version of Canonical Ubuntu Linux is installed on the remote host
- **DESCRIPTION**: According to its version, Canonical Ubuntu Linux is 8.04.x. It is, therefore, no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities
- **SOLUTION**: Upgrade to a version of Canonical Ubuntu Linux that is currently supported
- **RISK FACTOR**: Critical
- **CVSS v3.0 Base Score**: 10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
- **PLUGIN OUTPUT**: tcp/80/www

• 32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

REFERENCE: CVE-2008-0166

- **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 packager 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.
- **SOLUTION**: Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated
- **RISK FACTOR**: Critical
- **CVSS v3.0 Base Score**: 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
- **PLUGIN OUTPUT**: tcp/22/ssh

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

REFERENCE: CVE-2008-0166

- **SYNOPSIS**: The remote SSL certificate uses a weak key
- **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 packager 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
- **SOLUTION**: Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated
- **RISK FACTOR**: Critical
- **CVSS v3.0 Base Score**: 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
- **PLUGIN OUTPUT**: tcp/25/smtp
  tcp/5432/postgresql

• 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.
- **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)
- **PLUGIN OUTPUT**: tcp/25/smtp
  tcp/5432/postgresql

• 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 OUTPUT**: tcp/5900/vnc

~~~

DESCRIZIONE DETTAGLIATA DELLE VULNERABILITÀ HIGH

• 136769 - ISC BIND Service Downgrade / Reflected DoS

REFERENCE: CVE-2020-8616

- **SYNOPSIS:** The remote name server is affected by Service Downgrade / Reflected DoS vulnerabilities
- **DESCRIPTION**: According to its self-reported version, the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities. This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response. An unauthenticated, remote attacker can exploit this to cause degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack.
- **SOLUTION**: Upgrade to the ISC BIND version referenced in the vendor advisory
- **RISK FACTOR**: Medium
- **CVSS v3.0 Base Score**: 8.6 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)
- **PLUGIN OUTPUT**: udp/53/dns

• 42256 - NFS Shares World Readable

- **SYNOPSIS:** The remote NFS server exports world-readable shares
- **DESCRIPTION**: The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range)
- **SOLUTION**: Place the appropriate restrictions on all NFS shares
- **RISK FACTOR**: Medium
- **CVSS v3.0 Base Score**: 7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
- **PLUGIN OUTPUT**: tcp/2049/rpc-nfs
~~~

- **42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)**

REFERENCE: CVE-2016-2183

- **SYNOPSIS**: The remote service supports the use of medium strength SSL ciphers
- **DESCRIPTION**: The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.
- **SOLUTION**: Reconfigure the affected application if possible to avoid use of medium strength ciphers
- **RISK FACTOR**: Medium
- **CVSS v3.0 Base Score**: 7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
- **PLUGIN OUTPUT**: tcp/25/smtp
  tcp/5432/postgresql

- **90509 - Samba Badlock Vulnerability**

REFERENCE: CVE-2016-2118

- **SYNOPSIS**: An SMB server running on the remote host is affected by the Badlock vulnerability
- **DESCRIPTION**: The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services
- **SOLUTION**: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later
- **RISK FACTOR**: Medium
- **CVSS v3.0 Base Score**: 7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)
- **PLUGIN OUTPUT**: tcp/445/cifs

- **10205 - rlogin Service Detection**

REFERENCE: CVE-1999-0651

- **SYNOPSIS**: The rlogin service is running on the remote host
- **DESCRIPTION**: The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.
- **SOLUTION**: Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead
- **RISK FACTOR**: High
- **CVSS v2.0 Base Score**: 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
- **PLUGIN OUTPUT**: tcp/513/rlogin

- **10245 - rsh Service Detection**

REFERENCE: CVE-1999-0651

- **SYNOPSIS**: The rsh service is running on the remote host
- **DESCRIPTION**: The rsh service is running on the remote host. This service is vulnerable since data is passed between the rsh client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files
- **SOLUTION**: Comment out the 'rsh' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead
- **RISK FACTOR**: High
- **CVSS v2.0 Base Score**: 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
- **PLUGIN OUTPUT**: tcp/514/rsh

~~~

DESCRIZIONE DETTAGLIATA DELLE VULNERABILITÀ HIGH

Per ulteriori informazioni tecniche sulle precedenti vulnerabilità e per l'analisi tecnica delle vulnerabilità Medium, Low e Info, si veda **l'Appendice A: Report di Scansione Nessus**

~~~

CONCLUSIONI

Come già evidenziato nel sommario, la scansione della macchina METASPLOITABLE ha rilevato un totale di 187 vulnerabilità. Di queste, **9 raggiungono il grado di CRITICAL.** Cinque delle vulnerabilità CRITICAL hanno un punteggio CVSS v3.0 Base Score di 10 su 10, a riprova della loro estrema pericolosità.

La valutazione complessiva del rischio, per la macchina METASPLOITABLE, è alto. Questo è dovuto al già citato elevato numero di vulnerabilità e dalla facilità di sfruttamento delle stesse. Da non sottovalutare poi il potenziale impatto dello sfruttamento di alcune vulnerabilità che, in alcuni casi, potrebbero portare **l'attaccante a prendere completo possesso della macchina**.

Per quanto detto, si raccomanda di procedere al più presto possibile alla correzione delle vulnerabilità CRITICAL e HIGH.

~~~

ALTRI DOCUMENTI

Per un elenco completo di tutte le vulnerabilità rilevate e i dettagli tecnici completi, consultare l'Appendice A: Report di Scansione Nessus.
~~~