

M3_W12D1

Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable, indicando come target solo le porte comuni.

Abbiamo utilizzato come metodo di scansione il «Basic Network Scan».

A valle del completamento della scansione, analizzeremo attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

Ultimata la scansione il target presenta:

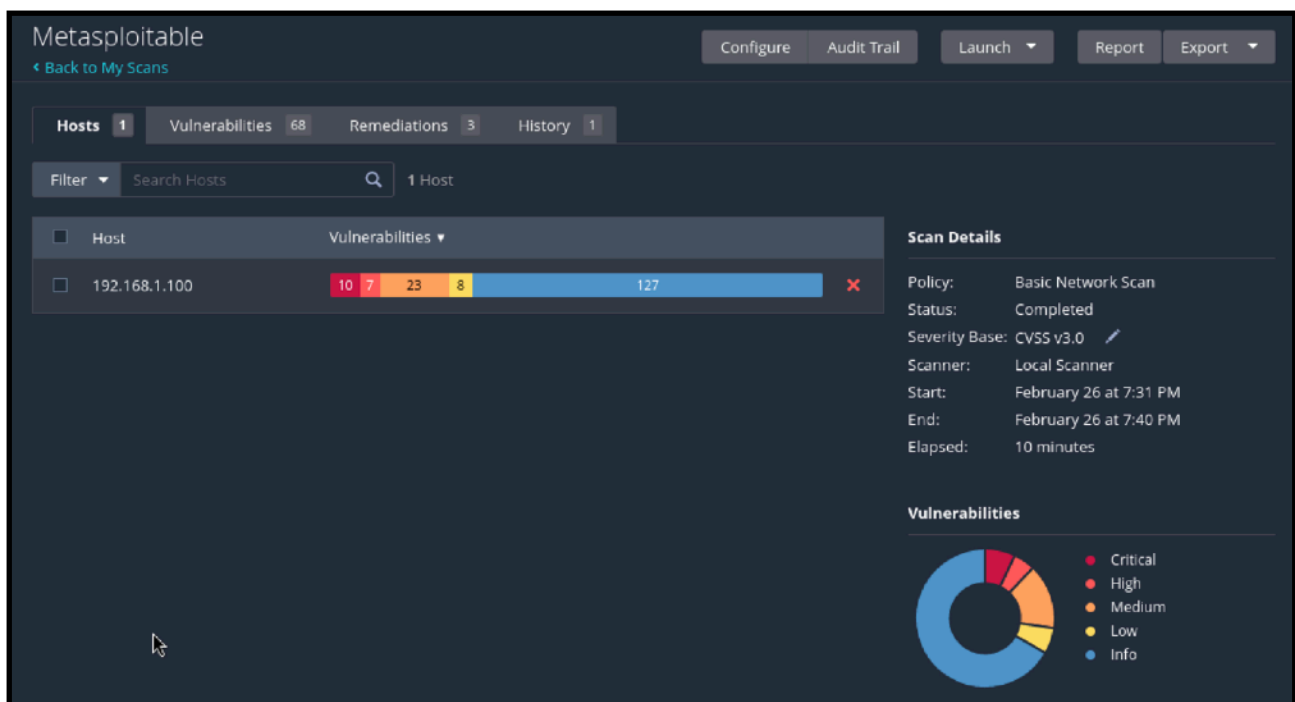
10 Critical Vulnerabilities

7 High Vulnerabilities

23 Medium Vulnerabilities

8 Low Vulnerabilities

127 Info System



Nessus mette a disposizione un Vulnerability Priority Rating (VPR) ed un Common Vulnerability Scoring System (CVSS). Sulla base di questi filtri quantificheremo il rischio associato ad ogni vulnerabilità e stabiliremo delle priorità per ogni remediation action da applicare.

Al primo posto per fattore di rischio legato alla criticità della vulnerabilità sul sistema target troviamo **UnrealRCd Backdoor Detection**: server Internet Relay Chat open source e dunque una backdoor che consentirebbe ad un malintenzionato la possibilità di eseguire comandi arbitrari sul server.
Soluzione: Per scongiurare il rischio dobbiamo installare una versione pulita e quindi aggiornata del software.

The screenshot shows the 'UnrealRCd Backdoor Detection' plugin details. The severity is 'Critical'. The description states that the remote IRC server is a version of UnrealRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host. The solution is to re-download the software, verify it using MD5 / SHA1 checksums, and re-install it. The 'See Also' section provides links to security advisories. The 'Output' section shows a terminal snippet: 'The remote IRC server is running as : uid=0 (root) gid=0 (root)'. The 'Port' table shows '6667 / tcp / irc' on host '192.168.1.100'. The 'Plugin Details' section lists: Severity: Critical, ID: 46882, Version: 1.16, Type: remote, Family: Backdoors, Published: June 14, 2010, Modified: April 11, 2022. The 'VPR Key Drivers' section lists: Threat Recency: No recorded events, Threat Intensity: Very Low, Exploit Code Maturity: Functional, Age of Vuln: 730 days +, Product Coverage: Low, CVSSV3 Impact Score: 5.9, Threat Sources: No recorded events. The 'Risk Information' section shows: Vulnerability Priority Rating (VPR): 7.4, Risk Factor: Critical.

Una vulnerabilità high-level riscontrata sul sistema target è **login Service Detection**: questo servizio rappresenta un'importante risorsa per l'attaccante poiché i dati transitano in chiaro in una comunicazione client-server. Un attacco con man-in-the-middle rende facilmente sfruttabile questa vulnerabilità che oltretutto può consentire accessi scarsamente autenticati senza password.
Soluzione: commentare la riga "login" in /etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilitare questo servizio e utilizzare SSH instead.

The screenshot shows the 'login Service Detection' plugin details. The severity is 'High'. The description states that 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. The solution is to comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead. The 'Output' section shows 'No output recorded.'. The 'Port' table shows '513 / tcp / rlogin' on host '192.168.1.100'. The 'Plugin Details' section lists: Severity: High, ID: 10205, Version: 1.36, Type: remote, Family: Service detection, Published: August 30, 1999, Modified: April 11, 2022. The 'VPR Key Drivers' section lists: Threat Recency: No recorded events, Threat Intensity: Very Low, Exploit Code Maturity: Unproven, Age of Vuln: 730 days +, Product Coverage: Low, CVSSV3 Impact Score: 5.9, Threat Sources: No recorded events. The 'Risk Information' section is present but empty.

Un'altra vulnerabilità high-leve altamente impattante per il nostro sistema target è **Samba Badlock Vulnerability**: questa versione è affetta da una falla, nota come Badlock, presente nei protocolli Security Account Manager (SAM) e Local Security Authority (Domain Policy) (LSAD). Un utente malintenzionato intercettando il traffico tra un client e una server che ospita un database SAM può sfruttare questa falla per forzare il declassamento del livello di autenticazione con lo scopo di modificare dati di sicurezza nel database Active Directory o la disabilitazione dei servizi critici.
Soluzione: Aggiornare Samba alla versione 4.2.11/4.3.8/4.4.2 o successive.

HIGH Samba 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 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.

See Also
<http://badlock.org>
<https://www.samba.org/samba/security/CVE-2016-2118.html>

Output

Plugin Details

Severity:	High
ID:	90509
Version:	1.8
Type:	remote
Family:	General
Published:	April 13, 2016
Modified:	November 20, 2019

VPR Key Drivers

Threat Recency:	No recorded events
Threat Intensity:	Very Low
Exploit Code Maturity:	Unproven
Age of Vuln:	730 days +
Product Coverage:	Medium
CVSSv3 Impact Score:	5.9
Threat Sources:	No recorded events

Vulnerabilità medium level importante da fixare **TLS Version 1.0 Protocol Detection**: questa versione presenta una serie di difetti di progettazione crittografica che potrebbe rivelarsi fatale durante il trasferimento di dati sensibili.
Soluzione: Abilitare TLS 1.2 e 1.3 e disabilitare TLS 1.0

MEDIUM TLS Version 1.0 Protocol Detection

Description
The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution
Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

See Also
<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

Plugin Details

Severity:	Medium
ID:	104743
Version:	1.10
Type:	remote
Family:	Service detection
Published:	November 22, 2017
Modified:	April 19, 2023

Risk Information

Risk Factor:	Medium
CVSS v3.0 Base Score:	6.5
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N
CVSS v2.0 Base Score:	6.1
CVSS v2.0 Vector:	CVSS2#AV:N/AC:H/Au:N/C:C/I:L/P:A/N

Un'altra vulnerabilità medium level riscontrata sul sistema target è **Unencrypted Telnet Server**: questo servizio su un canale non crittografato è altamente sconsigliato poiché login, password e comandi vengono trasferiti in chiaro. Soluzione: Disattivare il servizio Telnet e utilizzare SSH in quanto capace di proteggere le credenziali da intercettazioni aggiungendo flussi di dati aggiuntivi in grado di proteggere contenuti sensibili.

MEDIUM

Unencrypted Telnet Server

< >

Plugin Details

Description
The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution
Disable the Telnet service and use SSH instead.

Severity: Medium
ID: 42263
Version: 1.15
Type: remote
Family: Misc.
Published: October 27, 2009
Modified: January 16, 2024

Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score 6.5

E' altamente consigliato, indipendentemente dal livello di criticità, aggiornare ogni servizio che presenta vulnerabilità alla sua ultima versione oppure disattivarlo o sostituendolo con un servizio in grado di proteggere meglio qualsiasi tipo di dato sulla macchina qualora non fosse possibile eseguire un upgrade della versione.