

W12D4 - Pratica - parte due - remediation

Giacomo di Giacinto



W12D4 - Pratica PDF

Esercizio
Traccia e requisiti

Traccia:

Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità **critiche** e provate ad **implementare delle azioni di rimedio**.

N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio **per non più di una vulnerabilità**.

Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Ai fini della soluzione, abbiamo scelto le vulnerabilità in giallo nella figura in slide 3.

Consegna:

1. Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (tecnico, già riassunto) - **ScansioneInizio.pdf**
2. **Screenshot e spiegazione dei passaggi della remediation** - **RemediationMeta.pdf**
3. Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità (il grafico che mostra tutte le vulnerabilità) - **ScansioneFine.pdf**

Oppure un report unico, a vostra scelta. Penso sia più comodo farne tre comunque.

Nota: i report possono essere lasciati in inglese, senza problemi.

Se risolvete le 4 vulnerabilità, potete risolverne una quinta (a scelta), ad esempio con una regola di firewall

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Exported Share Information Disclosure
<input type="checkbox"/>	CRITICAL	10.0 *	rexecd Service Detection
<input type="checkbox"/>	CRITICAL	10.0	Unix Operating System Unsupported Version Detection
<input type="checkbox"/>	CRITICAL	10.0 *	VNC Server 'password' Password
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell Backdoor Detection

Di seguito saranno riportate le criticità oggetto di studio e la sua remediation.

CRITICAL

10.0*

5.9

11356

NFS Exported Share Information Disclosure

NFS Exported Share Information Disclosure

Language: English ▾

CRITICAL

Nessus Plugin ID 11356

[Information](#)[Dependencies](#)[Dependents](#)[Changelog](#)

Synopsis

It is possible to access NFS shares on the remote host.

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Plugin Details

Severity: Critical**ID:** 11356**File Name:** nfs_mount.nasl**Version:** 1.21**Type:** remote**Family:** RPC**Published:** 3/12/2003**Updated:** 8/30/2023**Supported Sensors:** Nessus

Sinossi

È possibile accedere alle condivisioni NFS sull'host remoto.

Descrizione

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un attaccante potrebbe essere in grado di sfruttare ciò per leggere (e eventualmente scrivere) file sull'host remoto.

Soluzione

Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

Remediation

Attraverso il comando da shell `sudo nano /etc/hosts.deny` posso negare l'accesso alle cartelle condivise. Modifico il file inserendo l'IP di kali in modo da negare l'accesso e porre rimedio alla criticità

```
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: some.host.name, .some.domain
#              ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
```

192.168.1.100

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

CRITICAL

10.0* - 61708

VNC Server 'password' Password

VNC Server 'password' Password

Language: English

CRITICAL

Nessus Plugin ID 61708

Information

Dependencies

Dependents

Changelog

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.

Plugin Details

Severity: Critical

ID: 61708

File Name: vnc_password_password.nasl

Version: Revision: 1.2

Type: remote

Family: [Gain a shell remotely](#)

Published: 8/29/2012

Updated: 9/24/2015

Supported Sensors: Nessus

Sinossi

Un server VNC in esecuzione sull'host remoto è protetto con una password debole.

Descrizione

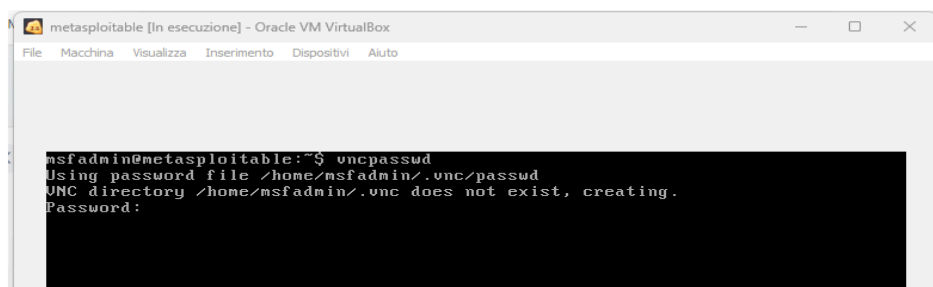
Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è stato in grado di effettuare il login utilizzando l'autenticazione VNC e una password 'password'. Un attaccante remoto e non autenticato potrebbe sfruttare ciò per prendere il controllo del sistema.

Soluzione

Proteggi il servizio VNC con una password forte.

Remediation:

Dovrà essere inserita una password al servizio VNC con il comando **vncpasswd**



CRITICAL 9.8 - 51988 Bind Shell Backdoor Detection

Bind Shell Backdoor Detection

Language: English ▾

CRITICAL Nessus Plugin ID 51988

Information

Dependencies

Dependents

Changelog

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.

Plugin Details

Severity: Critical

ID: 51988

File Name: wild_shell_backdoor.nasl

Version: 1.10

Type: remote

Family: Backdoors

Published: 2/15/2011

Updated: 4/11/2022

Configuration: Enable thorough checks

Supported Sensors: Nessus

Sinossi

L'host remoto potrebbe essere stato compromesso.

Descrizione

Una shell è in ascolto sulla porta remota senza richiedere alcuna autenticazione. Un attaccante potrebbe utilizzarla connettendosi alla porta remota e inviando comandi direttamente.

Soluzione

Verificare se l'host remoto è stato compromesso e reinstallare il sistema se necessario.

Remediation:

Nessus ci segnala che sulla porta 1524 c'è una backdoor attiva.

```
(kali㉿kali)-[~]  
$ nc 192.168.1.246 1524  
root@metasploitable:/# id  
uid=0(root) gid=0(root) groups=0(root)  
root@metasploitable:/#
```

Creando una regola ad hoc sul firewall possiamo disporre che nessun utente possa accedere alla porta, oppure possiamo selezionare gli utenti autorizzati all'accesso.

HIGH

7.5

5.9

90509

Samba Badlock Vulnerability

Samba Badlock Vulnerability

Language: English ▾

HIGH

Nessus Plugin ID 90509

Information

Dependencies

Dependents

Changelog

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 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>

Plugin Details

Severity: High

ID: 90509

File Name: samba_badlock.nasl

Version: 1.8

Type: remote

Family: General

Published: 4/13/2016

Updated: 11/20/2019

Supported Sensors: Nessus

Risk Information

VPR

Risk Factor: Medium

Sinossi:

Un server SMB in esecuzione sull'host remoto è affetto dalla vulnerabilità Badlock.

Descrizione

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da una falla, nota come Badlock, che esiste nei protocolli Security Account Manager (SAM) e Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione del livello di autenticazione non corretta su canali di chiamata di procedura remota (RPC). Un attaccante man-in-the-middle che è in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un declassamento del livello di autenticazione, il che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come la visualizzazione o la modifica di dati di sicurezza sensibili nel database Active Directory (AD) o la disabilitazione di servizi critici.

Soluzione

Aggiornare alla versione di Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.

Vedi anche

<http://badlock.org>

<https://www.samba.org/samba/security/CVE-2016-2118.html>

Remediation:

Installare come da soluzione una versione aggiornata della versione di Samba.

MEDIUM6.5-42263Unencrypted Telnet Server

Unencrypted Telnet Server

Language: English

MEDIUMNessus Plugin ID 42263

Information

Dependencies

Dependents

Changelog

Synopsis

The remote Telnet server transmits traffic in cleartext.

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.

Plugin Details

Severity: Medium

ID: 42263

File Name: telnet_clear_text.nasl

Version: 1.15

Type: remote

Family: Misc.

Published: 10/27/2009

Updated: 1/16/2024

Supported Sensors: Nessus

Risk Information

Sommario

Il server Telnet remoto trasmette il traffico in testo non criptato.

Descrizione

L'host remoto sta eseguendo un server Telnet su un canale non crittografato.

L'utilizzo di Telnet su un canale non crittografato non è consigliato poiché i login, le password e i comandi vengono trasferiti in chiaro. Ciò consente a un attaccante remoto man-in-the-middle di intercettare una sessione Telnet per ottenere credenziali o altre informazioni sensibili e per modificare il traffico scambiato tra un client e un server.

SSH è preferibile rispetto a Telnet poiché protegge le credenziali dall'intercettazione e può tunnelare flussi di dati aggiuntivi come una sessione X11.

Soluzione

Disabilitare il servizio Telnet e utilizzare invece SSH.

Remediation:

L'azienda dovrà abbandonare l'utilizzo di telnet ed, al suo posto, utilizzare SSH