

# SCANSIONE VULNERABILITÀ

Andremo ad utilizzare Nessus, **Nessus** è uno strumento di fondamentale importanza nel mondo della cybersecurity. È uno **scanner di vulnerabilità** che analizza i tuoi sistemi informatici alla ricerca di possibili punti deboli che potrebbero essere sfruttati da black hacker.

- **Cerca falle:** Esamina attentamente software, sistemi operativi, configurazioni di rete e altri elementi alla ricerca di bug, configurazioni errate e altre vulnerabilità note.
- **Valuta i rischi:** Classifica le vulnerabilità in base alla loro gravità, fornendo informazioni dettagliate su come potrebbero essere sfruttate.
- **Genera report:** Produce report completi e comprensibili che mostrano chiaramente lo stato di sicurezza della tua rete.
- **Si aggiorna costantemente:** Viene continuamente aggiornato con nuove firme di vulnerabilità per garantire la massima protezione.

## Perché è così importante?

- **Prevenzione degli attacchi:** Identificando le vulnerabilità prima che gli hacker possano sfruttarle, Nessus ti permette di agire in modo proattivo per proteggere i tuoi sistemi.
- **Conformità alle normative:** Molte normative in materia di sicurezza informatica richiedono la scansione periodica delle vulnerabilità. Nessus può aiutarti a soddisfare questi requisiti.
- **Riduzione dei rischi:** Valutando il rischio associato a ciascuna vulnerabilità, puoi prioritizzare le attività di correzione e allocare le risorse in modo efficiente.
- **Miglioramento della sicurezza:** Nessus ti aiuta a mantenere una postura di sicurezza più solida, proteggendo i tuoi dati e la tua reputazione.

Lo scanner ha riscontrato diverse vulnerabilità tra qui 5 critiche.

Restore Session

Nessus Essentials / Folders

https://carmine.8834/#/scans/reports/6/hosts/2/vulnerabilities

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

tenableNessus EssentialsScansSettings

FOLDERS

My ScanskAll ScansTrash

RESOURCES

PoliciesPlugin RulesTerrascan

Tenable News

Ada.cx SSRF via Sentry Misconfiguration

Read More

metasploitable2 / 192.168.8.11

ConfigureAudit TrailLaunchReportExport

Vulnerabilities 68

FilterSearch Vulnerabilities68 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count		
CRITICAL	10.0 *	7.4	0.6988	UnrealIRCd Backdoor Detection	Backdoors	1		
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1		
CRITICAL	9.8	9.0	0.9728	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1		
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2		
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1		
CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3		
HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1		
HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1		
HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1		
HIGH	7.5			NFS Shares World Readable	RPC	1		
MIXED	...	...	...	SSL (Multiple Issues)	General	29		
MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	5		

Host Details

IP: 192.168.8.11  
MAC: 08:00:27:ED:3E:B1  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)  
Start: Today at 4:47 PM  
End: Today at 4:55 PM  
Elapsed: 8 minutes  
KB: [Download](#)

Vulnerabilities

Critical

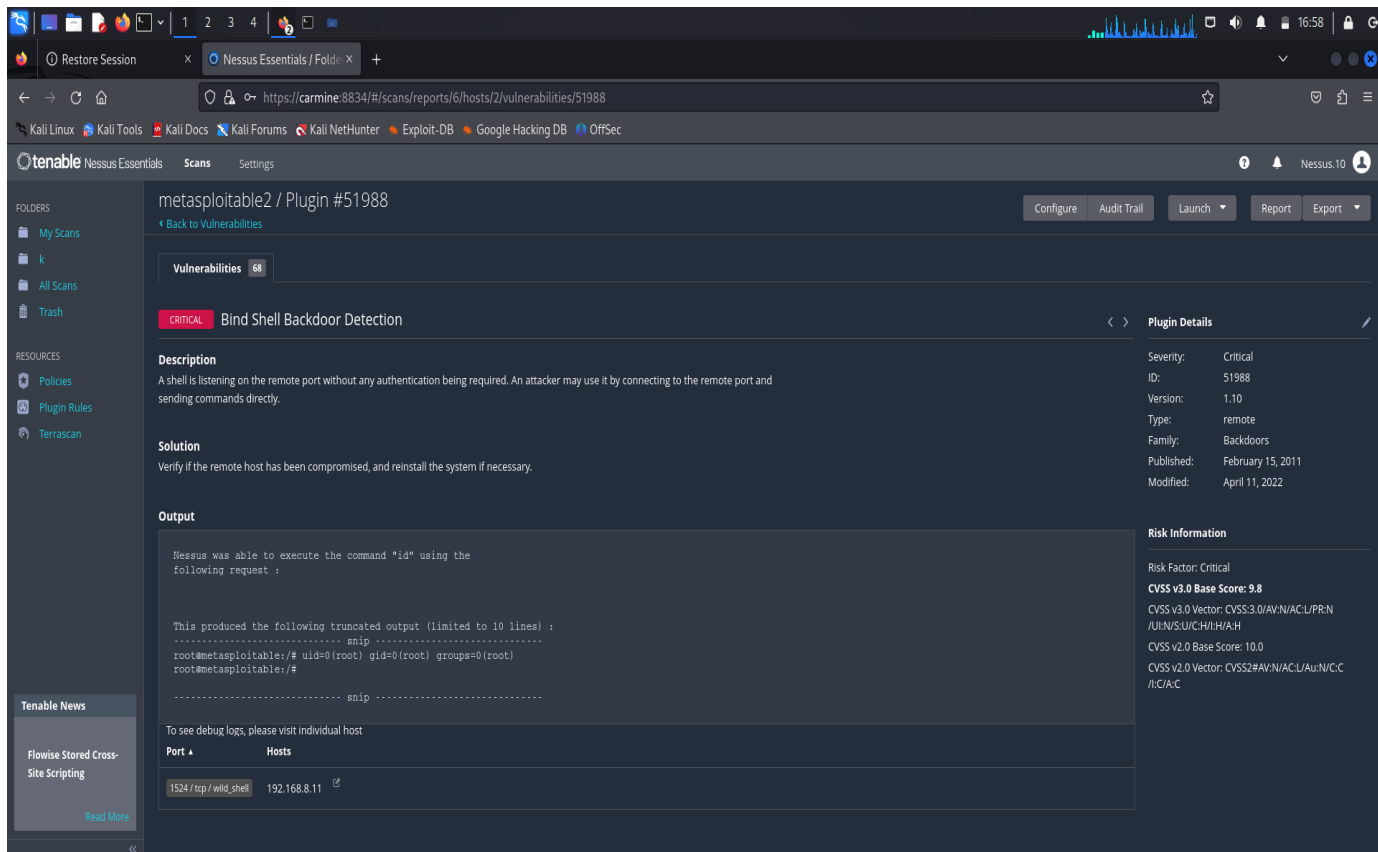
High

Medium

Low

Info

Bind Shell Backdoor Detection



## Descrizione:

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

## Soluzione

Verifica se l'host remoto è stato compromesso e, se necessario, reinstalla il sistema.

## Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

The screenshot displays the Nessus Essentials web interface. The browser address bar shows the URL: `https://carmine.8834/#/scans/reports/6/hosts/2/vulnerabilities/group/32321/32314`. The interface is in dark mode. On the left sidebar, there are sections for 'FOLDERS' (My Scans, k, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Tenable Scan). The main content area is titled 'metasploit2 / Plugin #32314'. Below this, there's a 'Vulnerabilities' section with a 'CRITICAL' status and the title 'Debian OpenSSH/OpenSSL Package Random Number Generator Weakness'. The 'Description' section explains that the remote SSH host key contains a bug in the OpenSSL library's random number generator. The 'Solution' section advises regenerating cryptographic material. The 'See Also' section provides links to Nessus advisories. The 'Output' section shows a table with one entry: '22/tcp / ssh' on host '192.168.8.11'. On the right, the 'Plugin Details' section lists metadata like Severity (Critical), ID (32314), and Version (1.21). Below that, 'VPR Key Drivers' shows threat metrics, and 'Risk Information' displays a VPR of 5.1 and a Risk Factor of Critical.

### Descrizione:

La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.

Il problema è dovuto al fatto che un packager Debian ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL.

Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man in the middle.

### Soluzione

Considera indovicabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

## Apache Tomcat AJP Connector Request Injection (Ghostcat)

The screenshot displays the Nessus Essentials web interface. The main content area shows the details for 'metasploitable2 / Plugin #134862'. The vulnerability is titled 'Apache Tomcat AJP Connector Request Injection (Ghostcat)' and is marked as 'CRITICAL'. The description states: '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)'. The solution provided is: '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.' The 'See Also' section lists several links to related Nessus advisories and CVEs. The 'Output' section shows a hex dump of the request used for exploitation. On the right, the 'Plugin Details' sidebar provides additional information: Severity: Critical, ID: 134862, Version: 1.46, Type: remote, Family: Web Servers, Published: March 24, 2020, Modified: July 17, 2024. The 'VPR Key Drivers' section lists threat recency, intensity, maturity, age, coverage, and impact scores. The 'Risk Information' section shows a Vulnerability Priority Rating (VPR) of 9.0, an Exploit Prediction Scoring System (EPSS) of 0.9728, a Risk Factor of High, and a CVSS v3.0 Base Score of 9.8.

**Description:**

È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni Web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice in modalità remota (RCE).

**Soluzione**

Aggiorna la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o successivo.

## VNC Server 'password' Password

The screenshot shows the Nessus Essentials web interface. The browser address bar displays the URL: `https://carmine:8834/#/scans/reports/6/hosts/2/vulnerabilities/61708`. The interface is in dark mode. On the left sidebar, there are sections for 'FOLDERS' (My Scans, k, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area is titled 'metasploitable2 / Plugin #61708'. Below this, there's a 'Vulnerabilities' section with a count of 68. The specific vulnerability is 'VNC Server 'password' Password', marked as 'CRITICAL'. The description states: '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.' The solution provided is: 'Secure the VNC service with a strong password.' The output section shows: 'Nessus logged in using a password of "password". To see debug logs, please visit individual host'. A table lists the host details: Port 5900 / tcp / vnc, Hosts 192.168.8.11. On the right, the 'Plugin Details' section shows: Severity: Critical, ID: 61708, Version: \$Revision: 1.2 \$, Type: remote, Family: Gain a shell remotely, Published: August 29, 2012, Modified: September 24, 2015. The 'Risk Information' section shows: Risk Factor: Critical, CVSS v2.0 Base Score: 10.0, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C. The 'Vulnerability Information' section shows: Default Account: true, Exploited by Nessus: true.

### Descrizione:

Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa situazione per assumere il controllo del sistema.

### Soluzione

Proteggi il servizio VNC con una password complessa.

## UnrealIRCd Backdoor Detection

The screenshot displays the Nessus Essentials web interface. The browser address bar shows the URL `https://carmine.8834/#/scans/reports/6/hosts/2/vulnerabilities/46882`. The page title is "metasploitable2 / Plugin #46882". The main content area shows a "CRITICAL" severity vulnerability titled "UnrealIRCd Backdoor Detection". The description states: "The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host." The solution provided is: "Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it." The "See Also" section lists three links: <https://seclists.org/fulldisclosure/2010/jun/277>, <https://seclists.org/fulldisclosure/2010/jun/284>, and <http://www.unrealircd.com/txt/unrealircdvisory.20100612.txt>. The "Output" section shows a snippet of a shell command: `uid=0 (root) gid=0 (root)`. The right-hand panel provides "Plugin Details" including Severity (Critical), ID (46882), Version (1.16), Type (remote), Family (Backdoors), Published (June 14, 2010), and Modified (April 11, 2022). It also lists "VPR Key Drivers" such as Threat Recency, Threat Intensity, and CVSSv3 Impact Score. The "Risk Information" section shows a Vulnerability Priority Rating (VPR) of 7.4, an Exploit Prediction Scoring System (EPSS) of 0.6988, and a Risk Factor of Critical.

Descrizione:

Il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente a un utente malintenzionato di eseguire codice arbitrario sull'host interessato.

Soluzione

Scaricare nuovamente il software, verificarlo utilizzando i checksum MD5/SHA1 pubblicati e reinstallarlo.