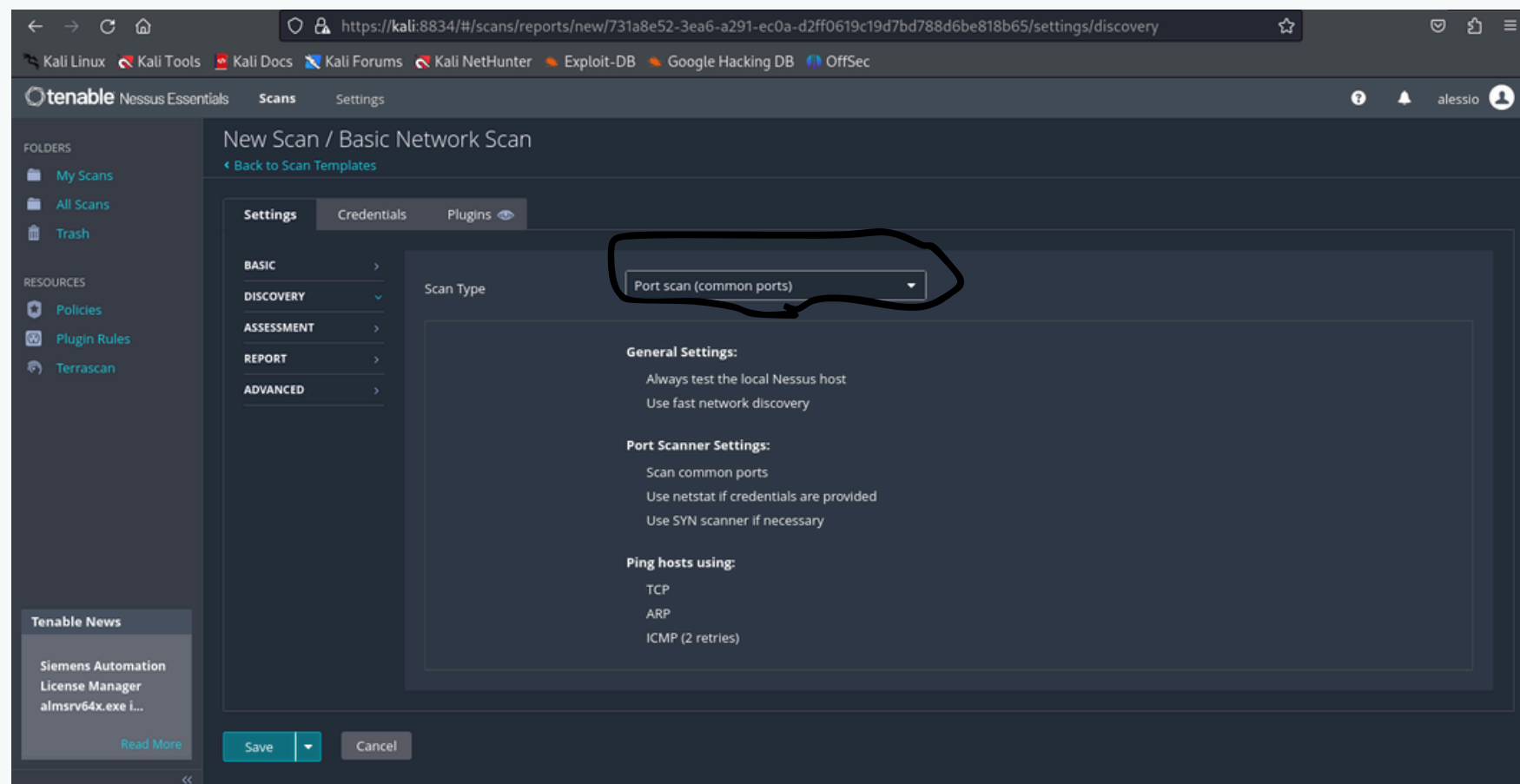


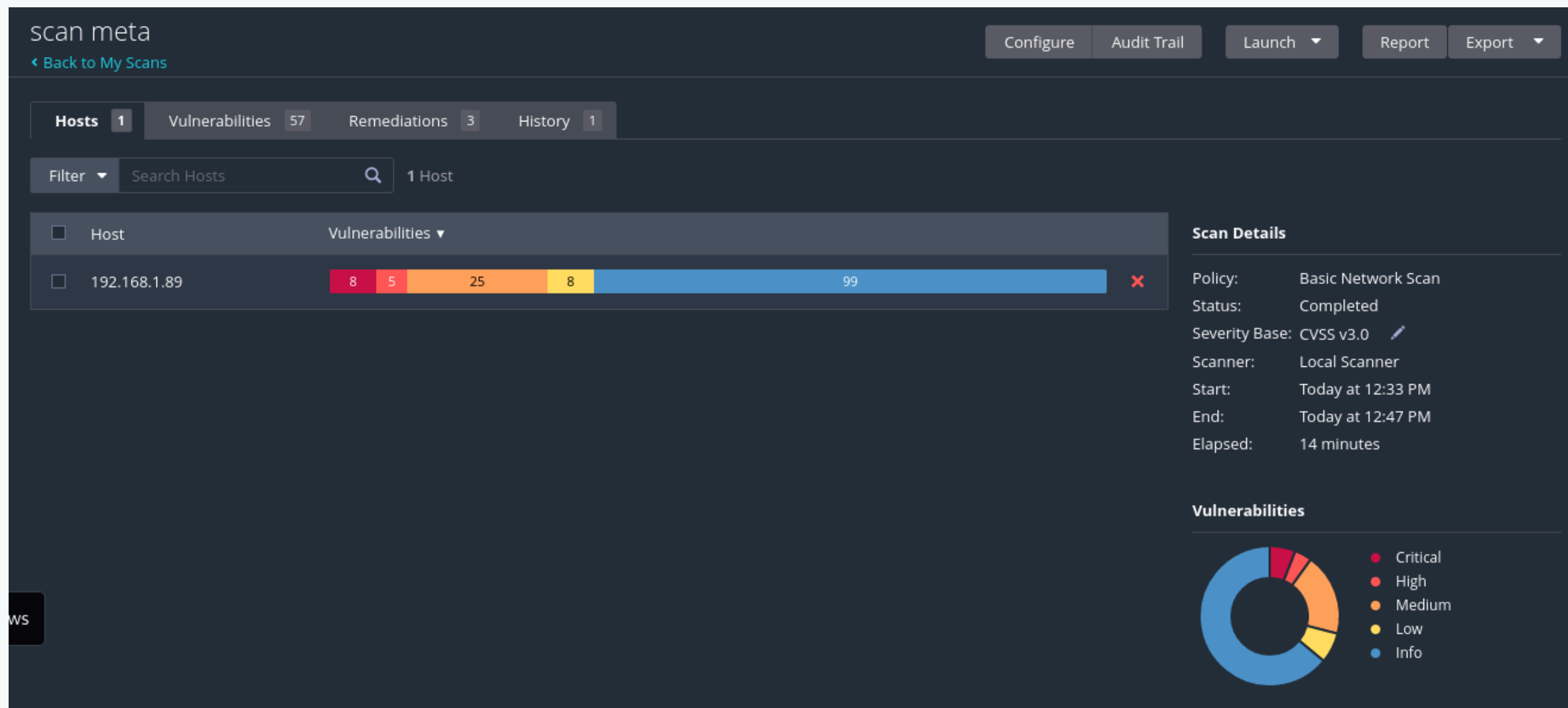
Pratica Nessus



Nessus è un popolare strumento di vulnerability assessment utilizzato per identificare vulnerabilità di sicurezza in reti, sistemi e applicazioni. Sviluppato da Tenable, Nessus è particolarmente apprezzato per la sua capacità di eseguire scansioni approfondite e generare report dettagliati sui rischi di sicurezza presenti in un ambiente IT.



**Inserimento dati Nessus per
scansionare le porte comuni di
Metasploitable**



**Avvio scansione del
programma per la ricerca
delle criticità**

Filter Search Vulnerabilities 57 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count		
CRITICAL	10.0 *	7.4	0.6988	UnrealIRCd Backdoor Detecti...	Backdoors	1		
CRITICAL	10.0 *			VNC Server 'password' Passw...	Gain a shell remotely	1		
CRITICAL	9.8	9.0	0.9728	Apache Tomcat AJP Connecto...	Web Servers	1		
CRITICAL	9.8			SSL Version 2 and 3 Protocol ...	Service detection	2		
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3		
HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1		
HIGH	7.5			NFS Shares World Readable	RPC	1		
MIXED	SSL (Multiple Issues)	General	28		
MIXED	ISC Bind (Multiple Issues)	DNS	5		
MEDIUM	6.5			TLS Version 1.0 P Plugin ID: 42263	Service detection	2		
MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1		
MEDIUM	5.9	4.4	0.9524	SSL DROWN Attack Vulnerabil...	Misc.	1		

Host Details

IP: 192.168.1.89
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 12:33 PM
End: Today at 12:47 PM
Elapsed: 14 minutes
KB: [Download](#)

Vulnerabilities

Critical

High

Medium

Low

Info

Alla fine della mia scansione avrò un report generale con tutti i livelli di criticità e consigli su come risolverli

Descrizione e soluzione delle criticità

scan meta / Plugin #32314

ConfigureAudit Trail

Back to Vulnerability Group

Vulnerabilities57

CRITICALDebian OpenSSH/OpenSSL Package Random Number Generator Weakness

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 particular, all SSH, SSL and OpenVPN key material should be re-generated.

See Also

<http://www.nessus.org/u?107f9bdc>
<http://www.nessus.org/u?f14f4224>

Output

No output recorded.

To see debug logs, please visit individual host

Descrizione

La chiave 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 causato da un pacchettizzatore Debian che ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL.

Un attaccante può facilmente ottenere la parte privata della chiave remota e utilizzare questa informazione per decifrare la sessione remota o per impostare un attacco man-in-the-middle.

Soluzione

Considera tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutte le chiavi SSH, SSL e OpenVPN dovrebbero essere rigenerate.

CRITICAL

UnrealIRCd Backdoor Detection

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also

<https://seclists.org/fulldisclosure/2010/jun/277>
<https://seclists.org/fulldisclosure/2010/jun/284>
<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

Output

The remote IRC server is running as :

uid=0(root) gid=0(root)

To see debug logs, please visit individual host

Port ▲	Hosts
6667 / tcp	192.168.1.89

Descrizione problema

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

soluzione

Proteggi il servizio VNC con una password forte.

Descrizione problema

La UnrealIRCd Backdoor è una vulnerabilità di tipo backdoor che colpisce UnrealIRCd, un noto software di IRC (Internet Relay Chat) server. Questa vulnerabilità è il risultato di una compromissione del codice sorgente in una versione specifica di UnrealIRCd, che includeva una backdoor nascosta. La backdoor consente a un attaccante remoto di eseguire comandi arbitrari sul server senza alcuna autenticazione, permettendogli di prendere il controllo completo del sistema vulnerabile.

Soluzione

Riscarica il software, verificane l'integrità utilizzando i checksum MD5 / SHA1 pubblicati (Stringhe di caratteri generate da algoritmi crittografici) e reinstallalo.

scan meta / Plugin #61708

ConfigureAudit

[Back to Vulnerabilities](#)

Vulnerabilities57

CRITICAL

VNC Server 'password' 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.

Output

Nessus logged in using a password of "password".

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.1.89



Descrizione

Il servizio remoto accetta connessioni crittate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diversi difetti crittografici, tra cui:

Uno schema di padding insicuro con cifrari CBC.

Schemi di rinegoziazione e ripristino della sessione insicuri.

Un attaccante può sfruttare queste vulnerabilità per condurre attacchi man-in-the-middle o per decriptare le comunicazioni tra il servizio interessato e i client.

Sebbene SSL/TLS disponga di un metodo sicuro per scegliere la versione più alta supportata del protocollo (in modo che queste versioni vengano utilizzate solo se il client o il server non supportano nulla di migliore), molti browser web implementano questo in modo non sicuro, consentendo a un attaccante di degradare una connessione (come nel caso del POODLE). Pertanto, si raccomanda di disabilitare completamente questi protocolli.

Il NIST ha stabilito che SSL 3.0 non è più accettabile per comunicazioni sicure. A partire dalla data di applicazione trovata nel PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di "crittografia forte" del PCI SSC.

Soluzione

Consulta la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0. Utilizza invece TLS 1.2 (con suite crittografiche approvate) o versioni superiori.

Descrizione

È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un attaccante remoto non autenticato potrebbe sfruttare questa vulnerabilità per leggere file dell'applicazione web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un attaccante potrebbe caricare codice JavaServer Pages (JSP) dannoso in diversi formati di file e ottenere l'esecuzione di codice remoto (RCE).

Soluzione

Aggiorna la configurazione AJP per richiedere l'autorizzazione e/o aggiorna il server Tomcat alla versione 7.0.100, 8.5.51, 9.0.31 o successive.

