



Nessus[®]
vulnerability scanner

ES S5L3 : Vulnerability Scanning

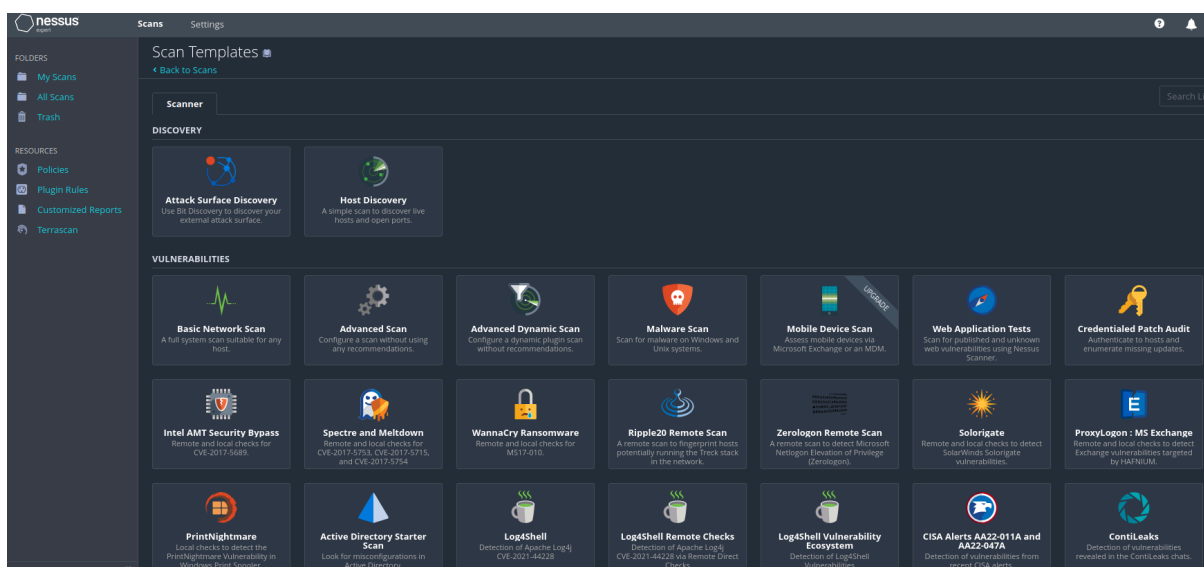
Che cos'è Nessus?

Nessus è uno strumento di scansione delle vulnerabilità usato per identificare falle di sicurezza in sistemi e reti informatiche. Sviluppato da Tenable, Nessus analizza dispositivi e applicazioni alla ricerca di punti deboli che potrebbero essere sfruttati da attacchi informatici, fornendo report dettagliati per aiutare gli amministratori a risolvere i problemi e proteggere l'infrastruttura.

Il database di vulnerabilità di Nessus viene aggiornato frequentemente da Tenable, il che consente a Nessus di rilevare le vulnerabilità più recenti e di mantenere l'accuratezza delle sue scansioni.

Il database contiene:

- Definizioni delle vulnerabilità (aggiornate regolarmente) con dettagli sulle debolezze conosciute, chiamate *plugin*.
- Risultati delle scansioni che mostrano i problemi rilevati sui dispositivi scansionati.
- Configurazioni di scansione che includono le impostazioni personalizzate dell'utente.

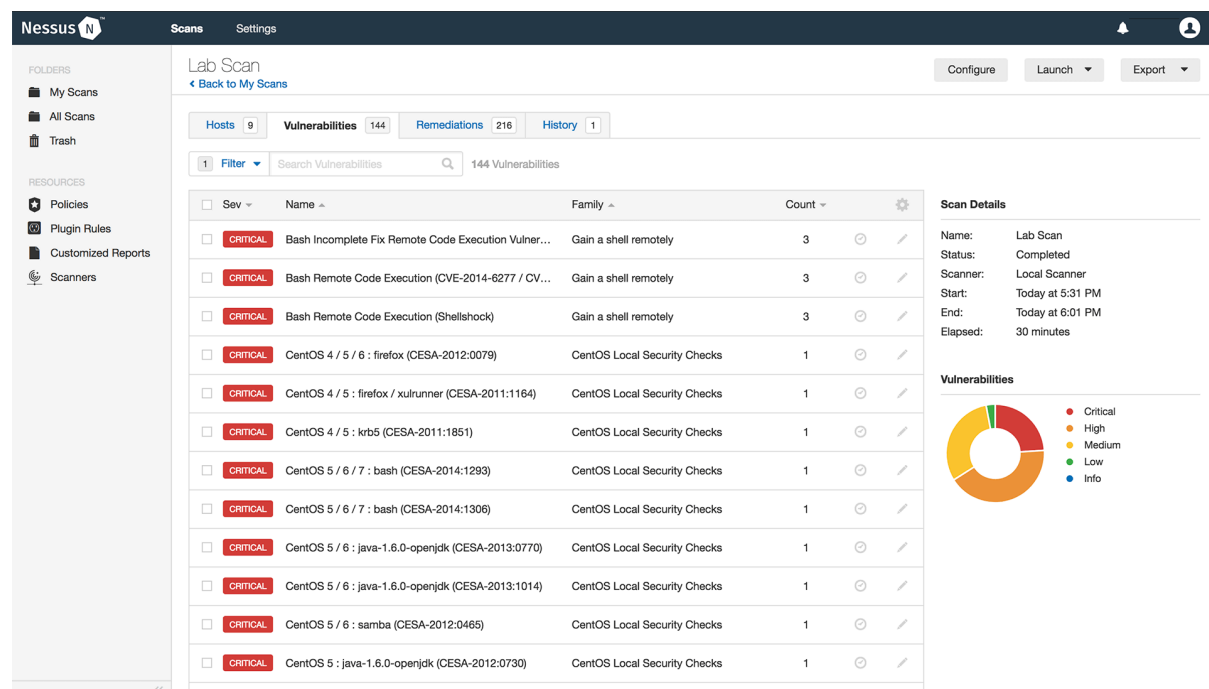


Interfaccia utente Nessus.

Cosa possiamo fare con nessus?

Con Nessus possiamo fare diverse attività di sicurezza informatica per proteggere sistemi e reti. Ecco le principali:

1. Scansione delle vulnerabilità: Identifica le debolezze in server, dispositivi di rete, e applicazioni, come software non aggiornato, configurazioni insicure e problemi noti.
2. Rilevamento di malware e backdoor: Scansiona i dispositivi per identificare segni di infezioni da malware o backdoor lasciate da potenziali attacchi.
3. Gestione delle patch: Fornisce informazioni su software obsoleti o vulnerabili, aiutando a identificare quali aggiornamenti (patch) sono necessari per rafforzare la sicurezza.
4. Reportistica e analisi dei rischi: Genera report dettagliati sui rischi di sicurezza presenti, con consigli su come risolverli, per supportare il team IT nella gestione delle vulnerabilità.



The screenshot shows the Nessus interface with the following details:

- Header:** Nessus logo, Scans, Settings, and user profile.
- Left Sidebar:** Folders (My Scans, All Scans, Trash) and Resources (Policies, Plugin Rules, Customized Reports, Scanners).
- Main Content:**
 - Lab Scan** header with a 'Back to My Scans' link.
 - Summary:** Hosts: 9, Vulnerabilities: 144, Remediations: 216, History: 1.
 - Filter:** Search Vulnerabilities (144 Vulnerabilities).
 - Vulnerability Table:**

Sev	Name	Family	Count
CRITICAL	Bash Incomplete Fix Remote Code Execution Vulner...	Gain a shell remotely	3
CRITICAL	Bash Remote Code Execution (CVE-2014-6277 / CV...	Gain a shell remotely	3
CRITICAL	Bash Remote Code Execution (Shellshock)	Gain a shell remotely	3
CRITICAL	CentOS 4 / 5 / 6 : firefox (CESA-2012:0079)	CentOS Local Security Checks	1
CRITICAL	CentOS 4 / 5 : firefox / xulrunner (CESA-2011:1164)	CentOS Local Security Checks	1
CRITICAL	CentOS 4 / 5 : krb5 (CESA-2011:1851)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 / 7 : bash (CESA-2014:1293)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 / 7 : bash (CESA-2014:1306)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:0770)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:1014)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : samba (CESA-2012:0465)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 : java-1.6.0-openjdk (CESA-2012:0730)	CentOS Local Security Checks	1
 - Scan Details:**
 - Name: Lab Scan
 - Status: Completed
 - Scanner: Local Scanner
 - Start: Today at 5:31 PM
 - End: Today at 6:01 PM
 - Elapsed: 30 minutes
 - Vulnerabilities:** A donut chart showing the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Esempio di analisi dei rischi (categorizzate secondo criteri di criticità).

Differenze tra Nmap e Nessus?

Nessus e Nmap sono entrambi strumenti di sicurezza informatica, ma hanno scopi e funzionalità diverse. Ecco le differenze principali:

1. Funzione principale:

- **Nessus:** È uno *scanner di vulnerabilità* progettato per identificare vulnerabilità di sicurezza in sistemi e reti, come software non aggiornato o configurazioni insicure.
- **Nmap:** È un *scanner di rete* che mappa e identifica dispositivi, porte aperte e servizi attivi su una rete, utile per la ricognizione e la scansione di porte.

2. Tipo di analisi:

- **Nessus:** Esegue scansioni approfondite per identificare specifiche vulnerabilità. Utilizza un database di *plugin* aggiornato per rilevare vulnerabilità note.
- **Nmap:** Si concentra sull'identificazione della struttura della rete, servizi, e porte aperte. Può fare una scansione superficiale di vulnerabilità, ma non è specifico per le vulnerabilità come Nessus.

3. Database di vulnerabilità:

- **Nessus:** Si basa su un database di vulnerabilità aggiornato regolarmente da Tenable(team di sviluppatori). Ogni vulnerabilità è associata a un *plugin*, che contiene dettagli specifici sulla minaccia.
- **Nmap:** Non ha un database di vulnerabilità ampio come Nessus.

4. Reportistica e gestione delle vulnerabilità:

- **Nessus:** Fornisce report dettagliati sui rischi, con suggerimenti per la risoluzione, e supporta la gestione delle vulnerabilità nel tempo.
- **Nmap:** È più orientato alla mappatura della rete e all'analisi di base; i report sono più semplici e spesso in formato grezzo.

5. Facilità d'uso e interfaccia:

- **Nessus:** Ha un'interfaccia grafica ed è orientato verso utenti aziendali e team di sicurezza, con opzioni avanzate di configurazione e reportistica.
- **Nmap:** Generalmente utilizzato da riga di comando, anche se esiste una GUI (*Zenmap*). È più flessibile per utenti esperti, ma ha una curva di apprendimento più ripida.

In sintesi, Nessus è ideale per la scansione delle vulnerabilità e la gestione dei rischi di sicurezza, mentre Nmap è principalmente uno strumento di mappatura della rete e di scoperta di porte e servizi.

Usiamo Nessus per eseguire un vulnerability test.

Nell'esercizio di oggi ci verrà chiesto di:

1. Configurazione della Scansione:

- Target: Metasploitable
- Porte: Solo le porte comuni (es. 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389)

Tipo di Scansione:

Puoi scegliere tra:

Basic Network Scan: Configurazione predefinita per una scansione di rete.

Advanced Scan: Configurabile in base alle tue esigenze specifiche.

2. Esecuzione della Scansione:

- Avvia la scansione configurata su Nessus.
- Attendi il completamento della scansione e assicurati che tutte le porte specificate siano state analizzate.

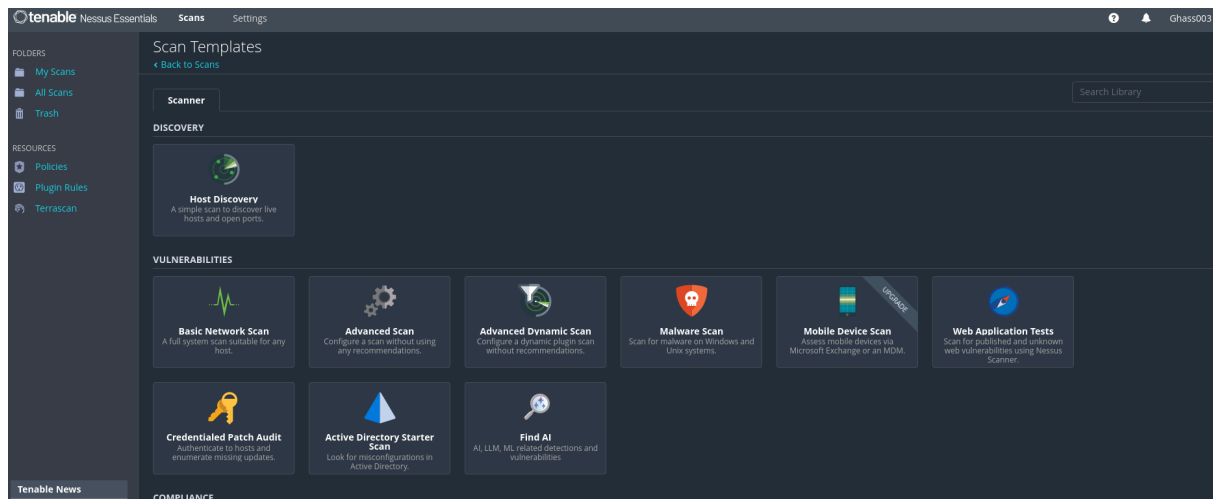
Configurazione della Scansione :

Partiamo innanzitutto con la configurazione di Nessus come obiettivo metasploitable.

Per fare questa configurazione ci serve sapere l'indirizzo IP del nostro Target , per questa volta ci verrà fornito ed è il seguente 192.168.43.101.

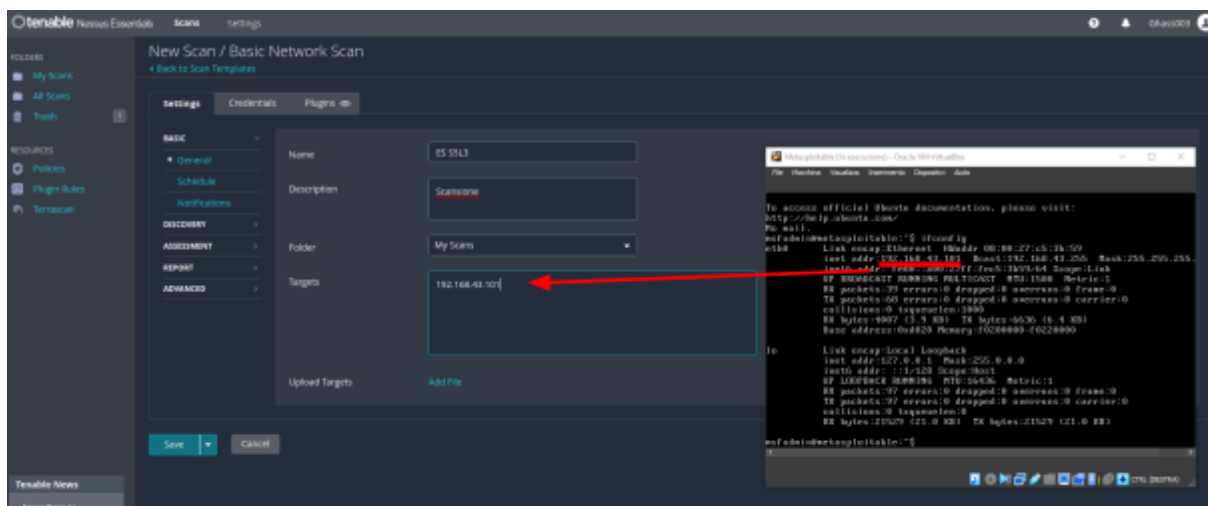
Ci dirigiamo nella nostra macchina virtuale di Kali linux e dopo aver installato Nessus inseriamo sulla barra di ricerca di un browser il seguente URL <https://kali:8834> inseriamo le nostre credenziali e continuiamo sull'interfaccia .

Una volta su Nessus clicchiamo su NEW SCAN e selezioniamo un plug in , in questo caso ci viene chiesto di eseguire un test sulla vulnerabilità . Clicchiamo su la prima voce su vulnerabilities .



Successivamente possiamo aprire Metasploitable (ricordiamoci che se è chiusa non funziona l'intero processo perché è come se l'host risultasse spento).

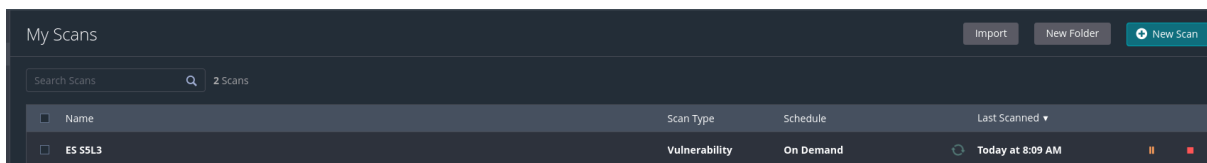
Lanciamo il comando "ifconfig" su Metasploitable per verificare l'IP . Una volta verificato possiamo proseguire su Nessus e inserire tutte le informazioni che ci vengono richieste, io ho deciso di fare una semplice Basic Network scan.



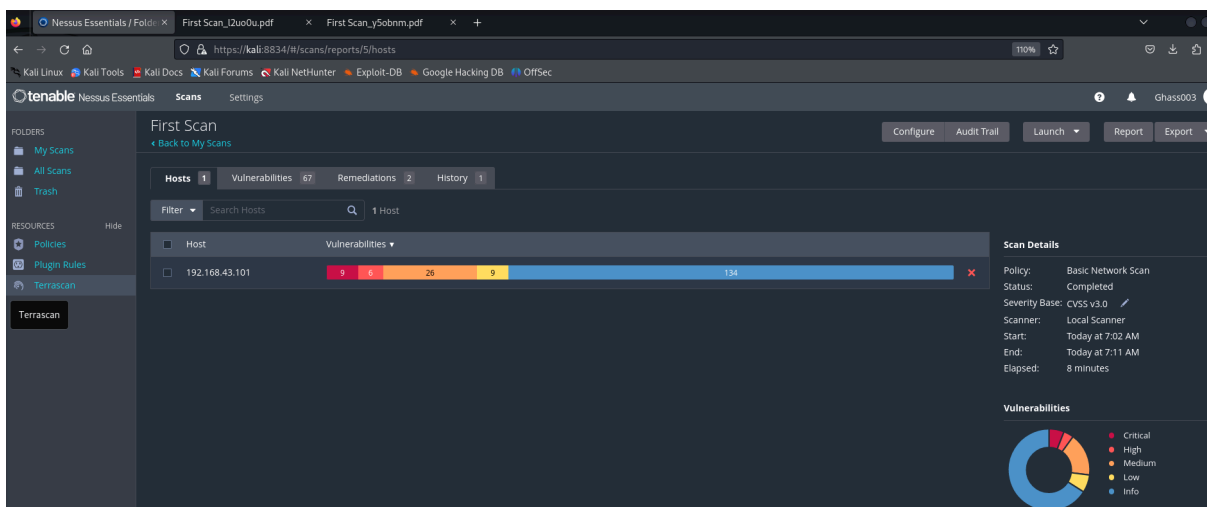
Esecuzione della scansione

Successivamente dopo aver riempito tutti i campi e aver verificato tutte le informazioni possiamo procedere con il Launch della nostra operazione. L'operazione potrebbe richiedere qualche minuto dipende molto dal nostro hardware e l'hardware che monta la macchina target perchè potrebbe risultare un'operazione pesante.

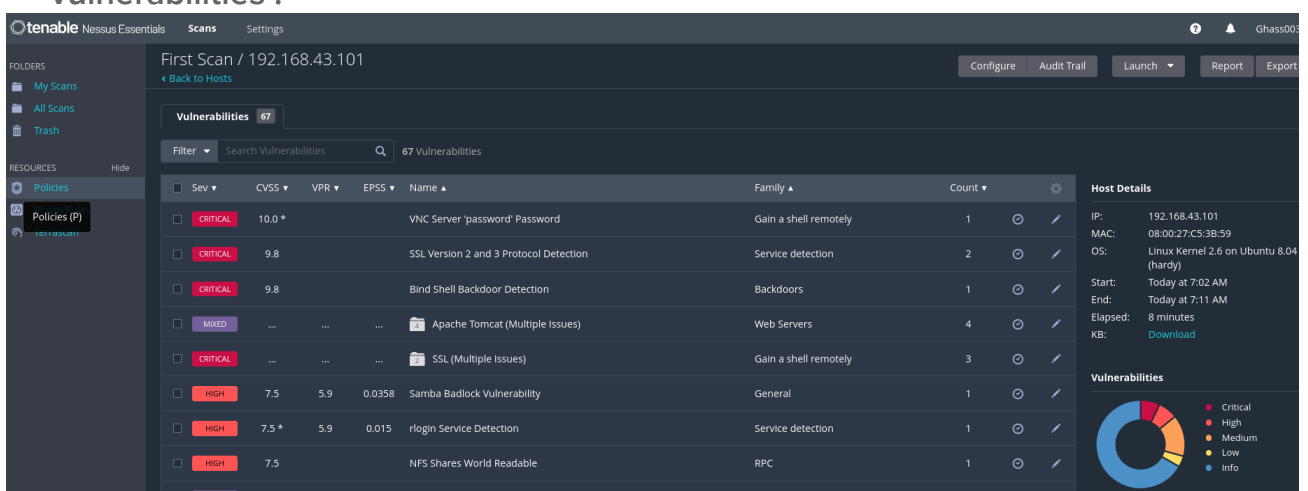
Possiamo tenere sotto supervisione l'operazione poichè Nessus ci offre a schermo la percentuale di avanzamento dell'operazione.



Una volta che l'operazione sarà terminata possiamo vedere che ci segnalerà il numero di vulnerabilità e ci darà una percentuale da quelle più critiche a quelle "innocue".



Possiamo vedere nel dettaglio tutte le vulnerabilità cliccando su vulnerabilities .



Analisi del Report

Dopo aver lanciato l'operazione siamo quasi giunti alla fine della nostra operazione, l'ultima operazione ovvero quella di analisi dei report a mio parere è la più cruciale perché potrebbe influire su tutta la rete aziendale o privata, se decidiamo di adottare soluzioni errate potremmo non solo danneggiare la rete ma anche gli host oppure mettere a rischio le informazioni e documenti aziendali.

Quindi un'attenta analisi dei report è fondamentale per portare a termine un'operazione di Penetration Test.

Delle soluzioni che possono tutelare il Pentester potrebbe essere quella di adottare una assicurazione sugli incidenti informatici.

A mio parere per aver un report che abbia tutte le informazioni necessarie per migliorare una vulnerabilità o molteplici è quella di implementare il nostro report con quello che ci fornisce Nessus.

Non avendo esperienza in campo ho provato a chiedere a chat quale sarebbe l'approccio migliore per avere un report efficiente e questi sono i punti che ha toccato:

Introduzione	Obiettivo del Report: Spiega lo scopo del penetration test e gli obiettivi specifici. Ambito del Test: Definisci i sistemi e le reti testate, con i limiti e le esclusioni. Strumenti Utilizzati: Elenca gli strumenti usati, includendo Nessus per la scansione delle vulnerabilità.
Metodologia	Fasi del Pentesting: Descrivi le fasi del test (ricognizione, scansione, enumerazione, sfruttamento, ecc.). Tecniche e Approcci: Spiega le tecniche adottate in ciascuna fase (es. scansione delle porte con Nmap, scansione delle vulnerabilità con Nessus).
Riepilogo dei Risultati	Riepilogo delle Vulnerabilità: Presenta un elenco delle vulnerabilità rilevate,

Riepilogo dei risultati.	<p>organizzate per livello di gravità (critico, alto, medio, basso).</p> <p>Impatto e Priorità: Sintetizza l'impatto delle vulnerabilità sul sistema, con una panoramica del livello di rischio complessivo.</p>
Dettaglio delle Vulnerabilità	<p>Vulnerabilità Chiave: Seleziona le vulnerabilità più critiche o rilevanti e analizzale in dettaglio.</p> <p>Descrizione: Descrizione della vulnerabilità e di come può essere sfruttata.</p> <p>Impatto: Impatto specifico sull'organizzazione.</p> <p>Prove (Evidence): Inserisci screenshot o dati di scansione da Nessus per supportare i risultati.</p> <p>Raccomandazioni: Suggerimenti su come risolvere la vulnerabilità (usa le raccomandazioni di Nessus come base).</p>
Analisi del Rischio	<p>Puoi includere una matrice dei rischi per rappresentare visivamente le vulnerabilità in base alla probabilità di sfruttamento e al loro impatto.</p>
Conclusioni e Raccomandazioni Generali	<p>Riassumi le principali vulnerabilità e suggerisci un piano di intervento prioritizzato. Qui, puoi fare affidamento sui suggerimenti di mitigazione di Nessus e formulare raccomandazioni per migliorare la sicurezza complessiva, come aggiornamenti di sistema, configurazioni sicure, o miglioramenti nei processi di monitoraggio.</p>
Allegati	<p>Allegare il report completo di Nessus (in PDF o HTML) può dare un livello aggiuntivo di dettaglio al tuo lavoro. Molte aziende apprezzano avere accesso diretto ai dati di Nessus per approfondire ogni singola vulnerabilità rilevata.</p> <p>Assicurati che i dettagli di Nessus siano comprensibili e contestualizzati rispetto alle necessità del tuo report finale.</p>

Analizziamo insieme le vulnerabilità :

Cliccando su una vulnerabilità ci verrà fuori il menu' dove possiamo selezionare una vulnerabilità critica .

The screenshot shows the Tenable Nessus Essentials interface. The main section displays a list of vulnerabilities for the host 192.168.43.101. The table includes columns for Severity, CVSS, VPR, EPSS, Name, Family, and Count. The vulnerabilities listed are:

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4
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			NFS Shares World Readable	RPC	1
MIXED	SSL (Multiple Issues)	General	28
MIXED	ISC Bind (Multiple Issues)	DNS	5

The right-hand panel shows host details for 192.168.43.101, including IP, MAC, OS, Start, End, Elapsed, and KB. It also features a 'Vulnerabilities' section with a donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Una volta sulla vulnerabilità possiamo vedere che Nessus ci dà molte informazioni , ci dice in questo caso che ci sono dei pattern insicuri , ci dice come un attaccante può eseguire un exploit ecc

Inoltre ci suggerisce una soluzione da adottare , in questo caso ci dice di aggiornare i servizi .

The screenshot shows the details of the 'ES SSL3 / Plugin #20007' vulnerability. The interface includes a header with the vulnerability name and a breadcrumb link. Below the header is a table of tabs for Hosts, Vulnerabilities, Remediations, and History. The main content area provides a detailed description of the vulnerability and a solution.

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.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

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.

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.

See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>

<http://www.nessus.org/u?b06c7e95>

<http://www.nessus.org/u?247c4540>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<http://www.nessus.org/u?5d15ba70>

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://tools.ietf.org/html/rfc7507>

<https://tools.ietf.org/html/rfc7568>

Oltre alle info sopra indicate possiamo vedere che ci da delle pagine web dove sono contenuti approfondimenti sull'argomento. Che possono aiutarci a trovare una soluzione ancora più efficace .

Output

```
- SSLv2 is enabled and the server supports at least one
Low Strength Ciphers (<= 64-bit key)
```

Name	Code	Key Size
EXP-RC2-CBC-MD5	0x00000000	128
EXP-RC4-MD5	0x00000000	128

more...

To see debug logs, please visit individual host

Port ▲	Hosts
25 / tcp / smtp	192.168.43.101

```
- SSLv3 is enabled and the server supports at least one
Explanation: TLS 1.0 and SSL 3.0 cipher suite
```

Medium Strength Ciphers (> 64-bit and < 112-bit key)

Name	Code	Key Size
EXP-RC2-CBC-MD5	0x00000000	128

more...

To see debug logs, please visit individual host

Port ▲	Hosts
5432 / tcp / postgresql	192.168.43.101

Nell'ultimo riquadro (l'output) vediamo le porte che interessano la vulnerabilità.

Per avere il report da Nessus possiamo cliccare su Report :

Generate Report - 1 Vulnerability Selected

Report Format: ☐ HTML ☒ PDF ☐ CSV

Select a Report Template:

SYSTEM

- Complete List of Vulnerabilities by Host
- Detailed Vulnerabilities By Host
- Detailed Vulnerabilities By Plugin
- Vulnerability Operations

Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:
None

Formatting Options:
☒ Include page breaks between vulnerability results

Generate Report Cancel Save as default

Ci verrà fuori una lista di report dove possiamo avere una relazione molto sintetica e una molto più dettagliata.

Ecco come si presenta il report semplificato :

First Scan

Report generated by Tenable Nessus™

Web, 30 Oct 2024 07:11:08 EDT

192.168.43.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
7	5	20	8	77

Vulnerabilities Total: 117

SEVERITY	CVEs V3.0	VPK SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9728	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	-	171340	Apache Tomcat SEOL (<= 5.5.x)
CRITICAL	10.0*	5.1	0.1175	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.1175	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	0.0164	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0358	90509	Samba Badlock Vulnerability
HIGH	7.5*	5.9	0.015	10205	rlogin Service Detection
MEDIUM	6.8	6.0	0.1176	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoni
MEDIUM	6.5	3.6	0.0041	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	42263	Unencrypted Telnet Server

192.168.43.101

Soluzioni che possiamo adattare alle criticità che abbiamo riscontrato :

Critical

1)SSL Version 2 and 3 Protocol Detection

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.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

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.

See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>

<http://www.nessus.org/u?b06c7e95>

<http://www.nessus.org/u?247c4540>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<http://www.nessus.org/u?5d15ba70>

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://tools.ietf.org/html/rfc7507>

<https://tools.ietf.org/html/rfc7568>

2)Bind Shell Backdoor Detection

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.

3)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>

4)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.

5)Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Description

The remote x509 certificate on the remote SSL server 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 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>