



# Cyber Security & E thical Hacking

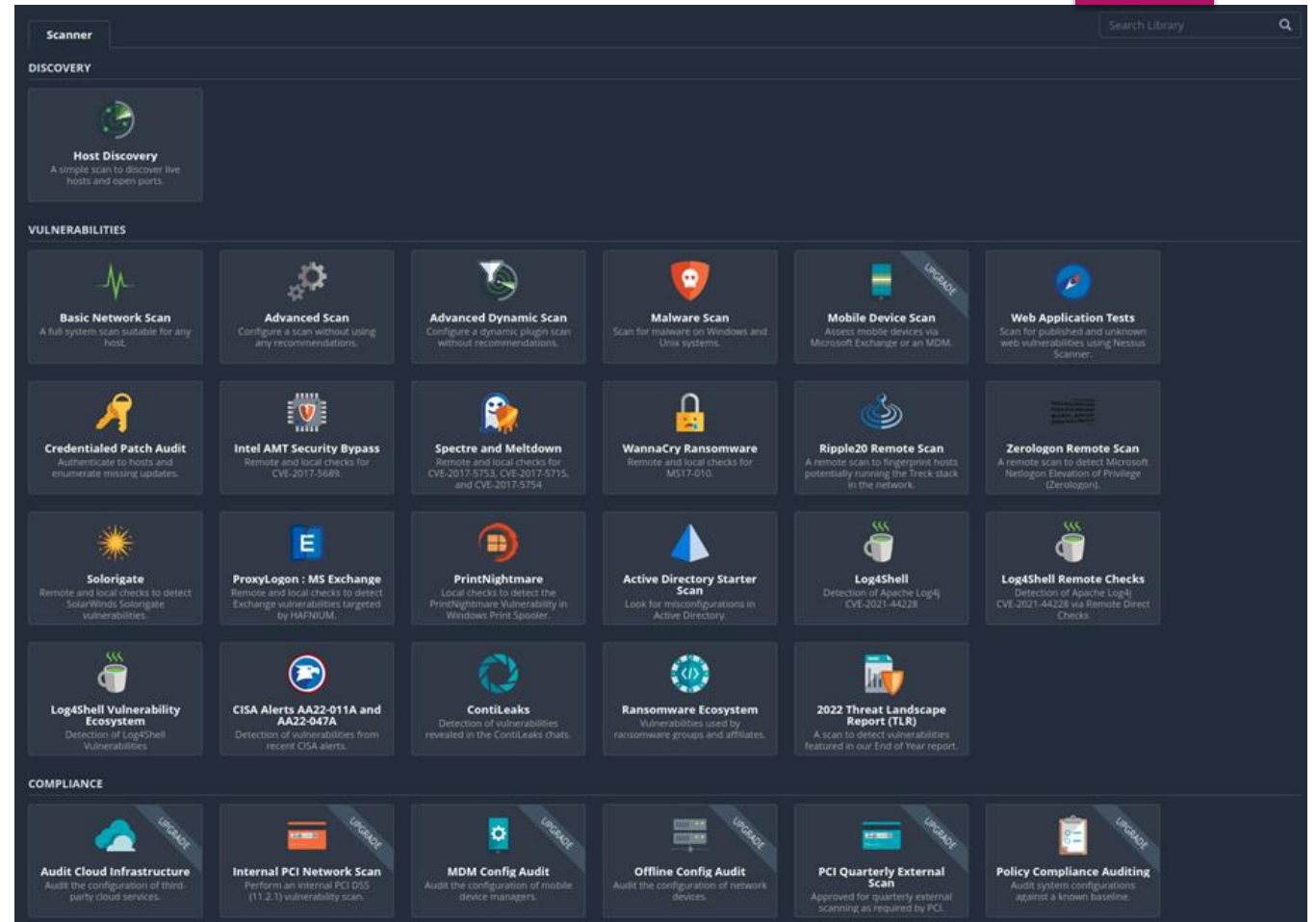
VALUTAZIONE DELLE  
VULNERABILITÀ



### Traccia

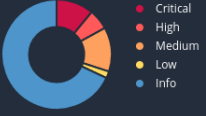
Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo). A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

► Nessus può eseguire scansioni approfondite dei sistemi, identificando potenziali vulnerabilità di sicurezza. Utilizza una vasta base di dati di vulnerabilità per confrontare le configurazioni dei sistemi e le versioni del software conosciute per problemi di sicurezza.





► Nessus assegna un punteggio di gravità alle vulnerabilità individuate, aiutandoti a concentrarti sulle aree che richiedono intervento immediato.

Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼			Host Details
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	🔄 ✎	<b>Host Details</b> IP: 192.168.50.101 MAC: 08:00:27:6C:D6:6B OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy) Start: Today at 4:01 PM End: Today at 4:35 PM Elapsed: 34 minutes KB: <a href="#">Download</a>
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	🔄 ✎	
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	🔄 ✎	
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	🔄 ✎	
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	🔄 ✎	<b>Vulnerabilities</b>  <ul style="list-style-type: none"> <li>● Critical</li> <li>● High</li> <li>● Medium</li> <li>● Low</li> <li>● Info</li> </ul>
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	🔄 ✎	
<input type="checkbox"/>	CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3	🔄 ✎	
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC	1	🔄 ✎	
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	🔄 ✎	
<input type="checkbox"/>	MIXED	...	...	SSL (Multiple Issues)	General	28	🔄 ✎	
<input type="checkbox"/>	MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5	🔄 ✎	
<input type="checkbox"/>	MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	🔄 ✎	
<input type="checkbox"/>	MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1	🔄 ✎	
<input type="checkbox"/>	MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and W...	Misc.	1	🔄 ✎	
<input type="checkbox"/>	MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1	🔄 ✎	
<input type="checkbox"/>	MIXED	...	...	SSH (Multiple Issues)	Misc.	6	🔄 ✎	
<input type="checkbox"/>	MIXED	...	...	SMB (Multiple Issues)	Misc.	2	🔄 ✎	
<input type="checkbox"/>	MIXED	...	...	TLS (Multiple Issues)	Misc.	2	🔄 ✎	
<input type="checkbox"/>	MIXED	...	...	TLS (Multiple Issues)	SMTP problems	2	🔄 ✎	

# CRITICAL

**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	192.168.50.101 <a href="#">🔗</a>

► Il server VNC in esecuzione sull'host remoto presenta una vulnerabilità in quanto la password utilizzata è debole. Nessus è stato in grado di effettuare l'accesso sfruttando l'autenticazione VNC con una password predefinita di 'password'. Questa falla potrebbe essere sfruttata da un attaccante remoto non autenticato per assumere il controllo del sistema.

► Soluzione: Rafforzare la sicurezza del servizio VNC mediante l'utilizzo di una password più robusta.

# CRITICAL

► Una shell è attiva su una porta remota senza richiedere alcuna forma di autenticazione. Questo apre la possibilità per un potenziale aggressore di sfruttare la situazione collegandosi alla porta remota e inviando comandi direttamente.

► Soluzione: Effettuare una verifica per determinare se l'host remoto è stato compromesso e, se necessario, procedere con la reinstallazione del sistema.

**CRITICAL** 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.

**Output**  
Nessus was able to execute the command "id" using the following request :  
  
This produced the following truncated output (limited to 10 lines) :  
..... snip .....  
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)  
root@metasploitable:/#  
..... snip .....  
  
To see debug logs, please visit individual host

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.50.101

- ▶ Il servizio remoto accetta connessioni crittografate tramite TLS 1.0. TLS 1.0 presenta alcune vulnerabilità di progettazione crittografica. Le implementazioni moderne di TLS 1.0 attenuano tali problematiche, ma versioni più recenti come 1.2 e 1.3 sono progettate per mitigare tali difetti e dovrebbero essere utilizzate ogni volta che possibile.
- ▶ A partire dal 31 marzo 2020, gli endpoint non abilitati per TLS 1.2 e versioni superiori non funzioneranno correttamente con i principali browser web e fornitori di servizi.
- ▶ Il PCI DSS v3.2 richiede che TLS 1.0 sia completamente disabilitato entro il 30 giugno 2018, ad eccezione dei terminali POS POI (e dei punti di terminazione SSL/TLS a cui si connettono) che possono essere verificati come non suscettibili a exploit noti.
- ▶ Soluzione: Abilitare il supporto per TLS 1.2 e 1.3, e disabilitare il supporto per 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>

**Output**

```
TLSv1 is enabled and the server supports at least one cipher.
```

To see debug logs, please visit individual host

Port ▲	Hosts
5432 / tcp / postgresql	192.168.50.101 <a href="#">🔗</a>
25 / tcp / smtp	192.168.50.101 <a href="#">🔗</a>