



NESSUS



COS'E'?

E' un vulnerability scanner, un software che esegue scansioni alla ricerca di vulnerabilità conosciute. Grazie al confronto con un database online o offline (meno aggiornato).




3 Fasi principali:

- 1) Invia un pacchetto: scopre che S.O. c'è e scansiona i programmi.
- 2) Li confronta e dà una valutazione.
- 3) E' la parte attiva: simula attacchi.


























Panoramica delle scannerizzazioni



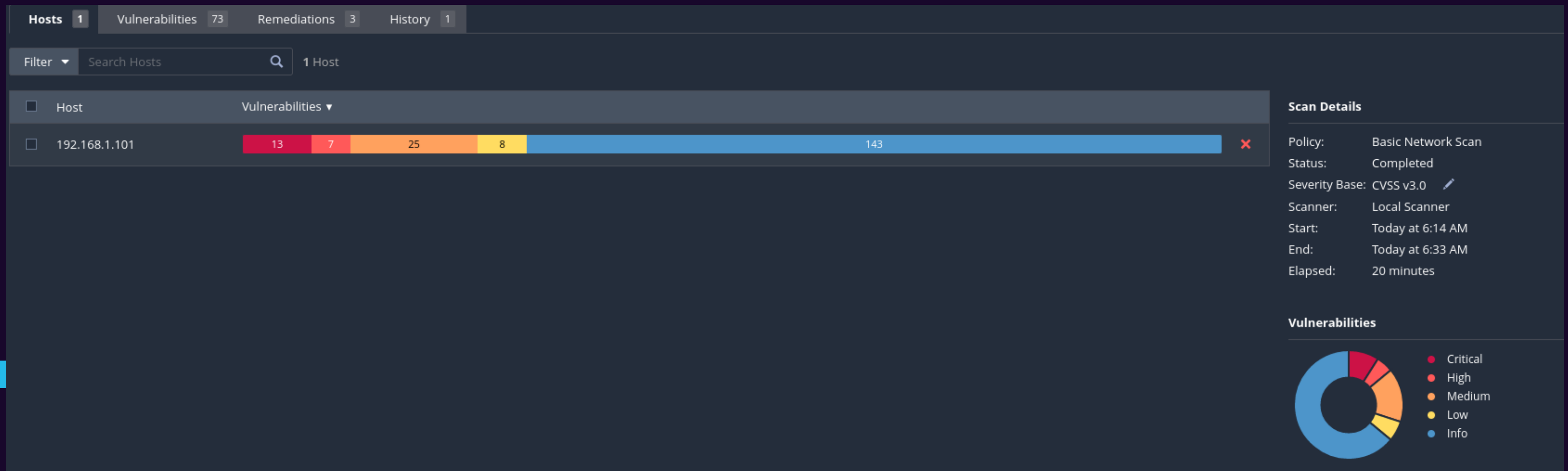
Host Discovery
A simple scan to discover live hosts and open ports.

VULNERABILITIES

 <p>Basic Network Scan A full system scan suitable for any host.</p>	 <p>Advanced Scan Configure a scan without using any recommendations.</p>	 <p>Advanced Dynamic Scan Configure a dynamic plugin scan without recommendations.</p>	 <p>Malware Scan Scan for malware on Windows and Unix systems.</p>	 <p>Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM.</p>	 <p>Web Application Tests Scan for published and unknown web vulnerabilities using Nessus Scanner.</p>	 <p>Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.</p>
 <p>Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.</p>	 <p>Spectre and Meltdown Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.</p>	 <p>WannaCry Ransomware Remote and local checks for MS17-010.</p>	 <p>Ripple20 Remote Scan A remote scan to fingerprint hosts potentially running the Treck stack in the network.</p>	 <p>Zerologon Remote Scan A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).</p>	 <p>Solorigate Remote and local checks to detect SolarWinds Solorigate vulnerabilities.</p>	 <p>ProxyLogon : MS Exchange Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.</p>
 <p>PrintNightmare Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.</p>	 <p>Active Directory Starter Scan Look for misconfigurations in Active Directory.</p>	 <p>Log4Shell Detection of Apache Log4j CVE-2021-44228</p>	 <p>Log4Shell Remote Checks Detection of Apache Log4j CVE-2021-44228 via Remote Direct Checks</p>	 <p>Log4Shell Vulnerability Ecosystem Detection of Log4Shell Vulnerabilities</p>	 <p>CISA Alerts AA22-011A and AA22-047A Detection of vulnerabilities from recent CISA alerts.</p>	 <p>ContiLeaks Detection of vulnerabilities revealed in the ContiLeaks chats.</p>
 <p>Ransomware Ecosystem Vulnerabilities used by ransomware groups and affiliates.</p>	 <p>2022 Threat Landscape Report (TLR) A scan to detect vulnerabilities featured in our End of Year report.</p>					



Faremo una scannerizzazione di rete standard





Nel dettaglio...

<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General
<input type="checkbox"/>	CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC
<input type="checkbox"/>	HIGH	7.5 *	6.7	rlogin Service Detection	Service detection
<input type="checkbox"/>	HIGH	7.5 *	6.7	rsh Service Detection	Service detection
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability	General
<input type="checkbox"/>	MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection
<input type="checkbox"/>	MEDIUM	6.5		Unencrypted Telnet Server	Misc.
<input type="checkbox"/>	MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection
<input type="checkbox"/>	MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.
<input type="checkbox"/>	MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers
<input type="checkbox"/>	LOW	3.7	4.5	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.
<input type="checkbox"/>	LOW	2.6 *		X Server Detection	Service detection

<input type="checkbox"/>	INFO			Nessus SYN scanner	Port scanners
<input type="checkbox"/>	INFO			RPC Services Enumeration	Service detection
<input type="checkbox"/>	INFO			Service Detection	Service detection
<input type="checkbox"/>	INFO			IRC Daemon Version Detection	Service detection
<input type="checkbox"/>	INFO			OpenSSL Detection	Service detection
<input type="checkbox"/>	INFO			RMI Registry Detection	Service detection
<input type="checkbox"/>	INFO			Service Detection (GET request)	Service detection
<input type="checkbox"/>	INFO			Unknown Service Detection: Banner Retrieval	Service detection
<input type="checkbox"/>	INFO			AJP Connector Detection	Service detection
<input type="checkbox"/>	INFO			Backported Security Patch Detection (FTP)	General
<input type="checkbox"/>	INFO			Backported Security Patch Detection (WWW)	General
<input type="checkbox"/>	INFO			Common Platform Enumeration (CPE)	General
<input type="checkbox"/>	INFO			Device Type	General
<input type="checkbox"/>	INFO			Ethernet Card Manufacturer Detection	Misc.
<input type="checkbox"/>	INFO			Ethernet MAC Addresses	General
<input type="checkbox"/>	INFO			ICMP Timestamp Request Remote Date Disclosure	General

Plugin ID: 10719



Il server VNC (condivisione remota) in esecuzione è protetto da una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC i 'password'. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa situazione per assumere il controllo del sistema.

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

192.168.1.101





In base al numero di versione auto-segnalato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato.

La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

Soluzione
Eseguire l'aggiornamento a una versione del sistema operativo Unix attualmente supportata.

CRITICAL

Unix Operating System Unsupported Version Detection

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Output

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).  
Upgrade to Ubuntu 23.04 / LTS 22.04 / LTS 20.04 .  
  
For more information, see : https://wiki.ubuntu.com/Releases
```

To see debug logs, please visit individual host

Port ▲	Hosts
N/A	192.168.1.101

