

# Vulnerability Scanner

Oggi andremo ad utilizzare un vulnerability scanner molto potente: Nessus.

Questo tool professionale e preciso è tra i migliori in circolazione e ci permette di rilevare le vulnerabilità dei vari componenti di una rete.

Nelle prossime slide andremo a vedere i risultati , il report e le azioni consigliate





# Il tool

Nessus è uno dei più diffusi scanner di vulnerabilità di rete e strumenti di valutazione della sicurezza. È progettato per aiutare le organizzazioni a individuare e risolvere le vulnerabilità nei propri sistemi informatici, dispositivi di rete e applicazioni.

Le principali caratteristiche di Nessus includono:

1. Scansione delle Vulnerabilità: Nessus esegue scansioni delle reti e dei sistemi per individuare vulnerabilità conosciute, che possono includere difetti del software, configurazioni errate e problemi di sicurezza. Fornisce informazioni dettagliate su ciascuna vulnerabilità scoperta.
2. Architettura dei Plugin: Nessus utilizza un'architettura basata su plugin, che consente di essere regolarmente aggiornato con nuovi controlli di vulnerabilità e controlli di conformità. Ciò assicura che Nessus sia sempre aggiornato con le ultime minacce e vulnerabilità di sicurezza.
3. Verifica della Conformità: Nessus può valutare i sistemi rispetto a diversi standard di conformità e politiche, come le linee guida CIS (Center for Internet Security), gli standard DISA STIGs (Security Technical Implementation Guides) e altro.
4. Reporting: Nessus genera report dettagliati che forniscono informazioni sulle vulnerabilità individuate, la loro gravità e raccomandazioni per la risoluzione. Questi report sono fondamentali per le squadre IT e di sicurezza per prioritizzare e affrontare i problemi di sicurezza.
5. Scansione con Credenziali: Nessus può effettuare scansioni autenticate, il che significa che può effettuare il login sui sistemi di destinazione con le credenziali appropriate e valutarli in modo più completo, inclusi problemi di configurazione e patch mancanti.
6. Personalizzazione: Gli utenti possono personalizzare le proprie scansioni specificando il tipo di scansioni, i sistemi di destinazione e altri parametri. Questa flessibilità consente alle organizzazioni di adattare Nessus alle proprie esigenze specifiche.

# Vediamo ora come si presenta con i vari tool e una parte delle possibili scelte, noi andremo a selezionare la Basic Network Scan

The screenshot displays the Tenable Nessus Essentials web interface. The top navigation bar includes the Tenable logo, 'Nessus Essentials', and tabs for 'Scans' and 'Settings'. The user's name 'Massimo' is visible in the top right corner. On the left sidebar, under 'FOLDERS', there are links for 'My Scans', 'All Scans', and 'Trash'. Under 'RESOURCES', there are links for 'Policies', 'Plugin Rules', and 'Terrascan'. The main content area is divided into two sections: 'DISCOVERY' and 'VULNERABILITIES'. The 'VULNERABILITIES' section contains a grid of 14 scan options. The 'Basic Network Scan' is highlighted with a red circle. Below the main grid, there is a 'Tenable News' section featuring a news item about 'Moxa MXsecurity Unauthenticated Device Registratio...'. The grid of scan options includes:

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

Settings

Credentials

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

nome scan

Description

descrizlone

Folder

My Scans

Targets

192.168.1.14

Upload Targets

Add File

Settings

Credentials

Plugins

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Scan Type

Port scan (common ports)

Port scan (common ports)

Port scan (all ports)

Custom

Use fast network discovery

Port Scanner Settings:

Scan common ports

Use netstat if credentials are provided

Use SYN scanner if necessary

Ping hosts using:

TCP

ARP

ICMP (2 retries)

Settings

Credentials

Plugins

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Scan Type

Default

Default

Scan for known web vulnerabilities

Scan for all web vulnerabilities (quick)

Scan for all web vulnerabilities (complex)

Custom

Disable web application scanning

Save

Cancel

Qui abbiamo le principali schermata quando selezioniamo il basic network scan, come possiamo vedere andiamo a indicare il nome dello scan, un eventuale descrizione, la cartella dove andremo a salvare lo scan e in fine l'indirizzo IP del nostro target. Nelle altre due immagini possiamo vedere alcune impostazioni utili per lo scan come, come il tipo di scansione che andremo ad effettuare e la scelta sulle porte sulle quali andremo a lavorare

Questo è il risultato della nostra scansione, come si può ben vedere Nessus provvede anche a dividere le diverse vulnerabilità in base al livello di urgenza. C'è da dire che questo programma è molto intuitivo e ben organizzato. Mette a nostra disposizione anche ulteriori informazioni riguardo il target come possiamo vedere nell'immagine sottostante nella parte destra

scan / 192.168.1.14

[Back to Hosts](#)

Configure

Audit Trail

Launch

Report

Export

Vulnerabilities73

Filter

Search Vulnerabilities

73 Vulnerabilities

<input type="checkbox"/>	Sev	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/>	CRITICAL	10.0	10.0	Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP)	CGI abuses	4		
<input type="checkbox"/>	CRITICAL	10.0	10.0	Apache Log4Shell RCE detection via callback correlation (Direct Check RPCBIND)	RPC	1		
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1		
<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		Bind Shell Backdoor Detection	Backdoors	1		
<input type="checkbox"/>	MIXED	...	...	<div>4</div> DNS (Multiple Issues)	DNS	5		
<input type="checkbox"/>	MIXED	...	...	<div>4</div> Apache Tomcat (Multiple Issues)	Web Servers	4		
<input type="checkbox"/>	CRITICAL	...	...	<div>2</div> SSL (Multiple Issues)	Gain a shell remotely	3		
<input type="checkbox"/>	MIXED	...	...	<div>2</div> SSL (Multiple Issues)	Service detection	3		
<input type="checkbox"/>	CRITICAL	...	...	<div>2</div> Apache Log4j (Multiple Issues)	Misc.	2		
<input type="checkbox"/>	CRITICAL	...	...	<div>2</div> Apache Log4j (Multiple Issues)	Web Servers	2		

Host Details

IP:

192.168.1.14

DNS:

Host-004.homenet.telecomitalia.it

MAC:

08:00:27:F5:52:7D

OS:

Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Start:

Today at 7:07 AM

End:

Today at 7:20 AM

Elapsed:

13 minutes

KB:

[Download](#)

Vulnerabilities

Critical

High

Medium

Low

Info



Una volta che il nostro scan è completo e abbiamo un chiaro quadro della situazione non ci resta che andare a realizzare un report, tramite un tool di Nessus, e andarlo ad analizzare.

Qui ci rendiamo conto di che grande lavoro fa questo tool in quanto ci suggerisce anche le best pratiche consigliate per determinate vulnerabilità, ci consiglia sul come agire nei confronti di determinate problematiche e ci fornisce anche fonti di controllo e confronto delle nostre informazioni.

Nelle prossime slide andremo ad analizzare alcune di queste e indicheremo delle possibili soluzioni.

## Host Information

---

DNS Name: Host-004.homenet.telecomitalia.it  
Netbios Name: METASPLOITABLE  
IP: 192.168.1.14  
MAC Address: 08:00:27:F5:52:7D  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

## Vulnerabilities

### 156164 - Apache Log4Shell CVE-2021-45046 Bypass Remote Code Execution

## Synopsis

---

The version of Apache Log4j used on the remote server is affected by a remote code execution vulnerability.

## Description

---

A remote code execution vulnerability exists in Apache Log4j < 2.16.0 due to insufficient protections on message lookup substitutions when dealing with user controlled input. A remote, unauthenticated attacker can exploit this, via a web request to execute arbitrary code with the permission level of the running Java process.

Note that this bypass requires a non-default configuration. Only Pattern Layouts with a Context Lookup (for example, `$$${ctx:loginId}`) are vulnerable to this.

This plugin requires that both the scanner and target machine have internet access.

## See Also

---

<https://logging.apache.org/log4j/2.x/security.html>  
<https://www.lunasec.io/docs/blog/log4j-zero-day/>  
<http://www.nessus.org/u?a0e621e5>

## Solution

---

Upgrade to Apache Log4j version 2.16.0 or later, or apply the vendor mitigation.

Come possiamo vedere il report ci segnala che : Esiste una vulnerabilità legata all'esecuzione di codice in modalità remota in Apache Log4j < 2.16.0 a causa di protezioni insufficienti sulle sostituzioni di ricerca dei messaggi quando si tratta di input controllati dall'utente. Un utente malintenzionato remoto e non autenticato può sfruttare questa situazione, tramite una richiesta web per eseguire codice arbitrario con il livello di autorizzazione del processo Java in esecuzione.

Come sempre Nessus ci rimanda ad alcuni link da consultare per saperne di più riguardo questa problematica e ci da la possibile soluzione, ovvero aggiornare Apache Log4 alla versione 2.16.0 o successive

## 51988 - Bind Shell Backdoor Detection

### Synopsis

The remote host may have been compromised.

### 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.

### Risk Factor

Critical

### CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

### Plugin Output

tcp/1524/wild\_shell

```
Nessus was able to execute the command "id" using the
following request :
```

La seconda vulnerabilità che andiamo a prendere in considerazione riguarda la presenza di una shell che 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. Ben conosciamo i rischi legati alla presenza di backdoor, che possono essere sì uno strumento importante ma altrettanto pericoloso.

In questo caso la soluzione consigliata è verificare se l'host remoto è stato compromesso e, se necessario, reinstalla il sistema.



## 156016 - Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP)

### Synopsis

The remote web server is affected by a remote code execution vulnerability.

### Description

The remote web server is affected by a remote code execution vulnerability via a flaw in the Apache Log4j library. The vulnerability is due to the processing of unsanitized input sent to a logging function. A remote, unauthenticated attacker can exploit this, via a web request to execute arbitrary code with the permission level of the running Java process.

### See Also

<https://logging.apache.org/log4j/2.x/security.html>

<https://www.lunasec.io/docs/blog/log4j-zero-day/>

### Solution

Upgrade to Apache Log4j version 2.15.0 or later, or apply the vendor mitigation.

Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to <https://logging.apache.org/log4j/2.x/security.html> for the latest versions.

### Risk Factor

High

### CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

### CVSS v3.0 Temporal Score

La terza vulnerabilità :

Il server Web remoto è interessato da una vulnerabilità legata all'esecuzione di codice in modalità remota.

Il server Web remoto è affetto da una vulnerabilità legata all'esecuzione di codice in modalità remota tramite un difetto nella libreria Apache Log4j. La vulnerabilità è dovuta all'elaborazione di input non disinfettati inviati a una funzione di registrazione. Un utente malintenzionato remoto e non autenticato può sfruttare questa situazione, tramite una richiesta web per eseguire codice arbitrario con il livello di autorizzazione del processo Java in esecuzione.

Anche in questo caso la soluzione è aggiornare i driver di Apache

11356 - NFS Exported Share Information Disclosure

Synopsis	
It is possible to access NFS shares on the remote host.	
Description	
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.	
Solution	
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.	
Risk Factor	
Critical	
VPR Score	
5.9	
CVSS v2.0 Base Score	
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)	
References	
CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554
Exploitable With	
Metasploit (true)	

La quarta vulnerabilità che andiamo a prendere in esempio riguarda: La Divulgazione delle informazioni sulle condivisioni esportate da NFS. È possibile accedere alle condivisioni NFS sull'host remoto.

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto.

In questo caso la soluzione consigliata è:

Configura NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.



Fine.

Grazie.

Massimo Cinquegrana