

SCANSIONE COMPLETA SUL TARGET METASPLOITABLE

REPORTED BY
Benedetta
Forestieri



```
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417
```

```
    {  
        sort_order'];  
  
        SORT_ASC, $quotes);  
        ['shipping_methods'] = $quotes;  
        ['address'] = $address;  
  
        s->language->get('  
            _methods');  
        tes;  
  
        ta['lpa']['shipping_method']) && !  
        ta['lpa']['shipping_method']) &&  
        ['lpa']['shipping_method']['code']  
        ssion->data['lpa'][''
```

NESSUS

Per condurre scansioni di vulnerabilità utilizzo Nessus

Nessus è un **vulnerability scanner**. Mi consente di configurare e avviare diverse tipologie di scansioni attraverso il client, mentre il server si occupa dell'esecuzione e del confronto dei risultati con un database di riferimento.

Una volta installato, avvio il software utilizzando il seguente comando:

```
(betta@kali)-[~]  
$ sudo systemctl start nessusd.service
```

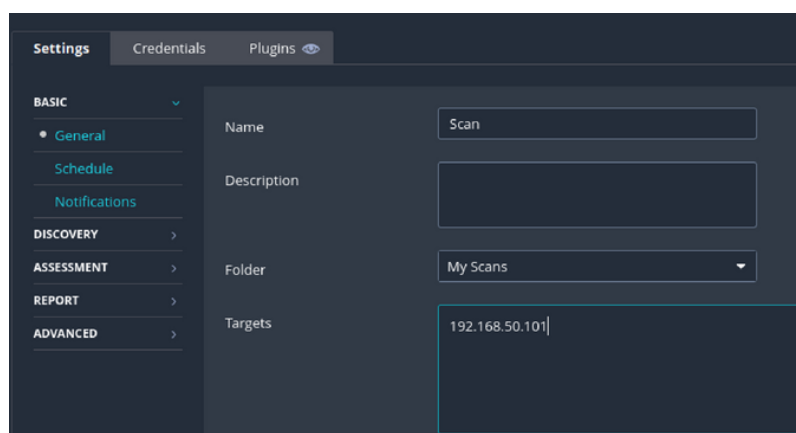
Dopo aver avviato, posso accedere all'interfaccia web di Nessus con l'indirizzo **https://kali:8834/**

Avvio una scansione inserendo l'ip di metasploitable in "target" ed imposto sulle porte comuni

La scansione mi informa delle varie vulnerabilità.

Decido di risolvere le seguenti:

- Bind Shell Backdoor Detection
- VNC Server 'password' Password
- NFS Exported Share Information Disclosure



Hosts 1 Vulnerabilities 60 Remediations 2 History 1


Filter Search Vulnerabilities 60 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
CRITICAL	10.0 *		V...	Gain a shell remotely	1	
CRITICAL	10.0		U...	General	1	
CRITICAL	10.0 *	5.9	N...	RPC	1	
CRITICAL	9.8		Bi...	Backdoors	1	
HIGH	7.5	6.7	S...	General	1	
HIGH	7.5		N...	RPC	1	
MEDIUM	6.5		T...	Service detection	2	
MEDIUM	5.9	4.4	S...	Misc.	1	Snooze

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 9:26 AM
End: Today at 10:01 AM
Elapsed: 35 minutes

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

Bind Shell Backdoor Detection

La vulnerabilità indica che c'è una porta sul server remoto in cui è possibile avviare una sessione di shell senza dover fornire un nome utente o una password.

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

Plugin Details

Severity: Critical

ID: 51988

Version: 1.10

Type: remote

Family: Backdoors

Published: February 15, 2011

Modified: April 11, 2022

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: 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

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

```
msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server start
sudo: /etc/init.d/nfs-kernel-server: command not found
msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server start
* Exporting directories for NFS kernel daemon... [ OK ]
* Starting NFS kernel daemon [ OK ]
msfadmin@metasploitable:~$
```

- *sudo su*: mi permette di diventare "root", fornendo accesso completo a tutte le funzionalità del sistema, consente di eseguire comandi come amministratore.
- *ufw enable*: abilito il servizio UFW (Uncomplicated Firewall) su un sistema. UFW è uno strumento di configurazione semplificato per il firewall in Linux. Quando attivato, il firewall inizia a filtrare il traffico di rete.
- *ufw default ALLOW*: il firewall consentirà tutto il traffico in entrata, a meno che non vengano specificate regole che lo vietano.
- *ufw deny 1524*: impedisco il traffico in ingresso sulla porta 1524

Per verificare se la chiusura della porta è andata a buon fine, utilizzo **Nmap**. Nmap è un **port scanner**, mette a disposizione metodi diversi di scansione delle porte degli host.

```
(betta@kali)-[~]
$ nmap -p 1524 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 14:27 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0076s latency).
PORT      STATE SERVICE
1524/tcp  filtered ingreslock
Nmap done: 1 IP address (1 host up) scanned in 13.33 seconds
```

Come si evince in figura, la porta è stata chiusa con successo. Dopo aver eseguito la scansione, la vulnerabilità non è più presente.

VNC Server 'password' Password

La vulnerabilità descritta riguarda un server VNC (Virtual Network Computing) che è stato configurato con una password debole (la password è "password"). Questo rende il sistema vulnerabile all'accesso non autorizzato, poiché un attaccante remoto e non autenticato potrebbe sfruttare questa debolezza 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	192.168.50.101

Plugin Details
Severity: Critical
ID: 61708
Version: \$Revision: 1.2 \$
Type: remote
Family: Gain a shell remotely
Published: August 29, 2012
Modified: September 24, 2015

Risk Information
Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:J/I:C/A:C

Vulnerability Information

La soluzione è procedere con un cambio password.

- Avvio la macchina virtuale Metasploitable, accedo con privilegi di amministratore usando il comando "sudo su".
- Utilizzo il comando "vncpasswd" per modificare la password VNC.
- Accedendo a Kali Linux con il comando "vncviewer" seguito dall'indirizzo IP di Metasploitable ho verificato che la modifica della password VNC è stata effettuata con successo.

```
(betta@kali)~[~/Desktop]
$ vncviewer 192.168.50.101
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password: VNC Server 'password' Password
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

NFS Exported Share Information Disclosure

Questa vulnerabilità critica riguarda una condivisione NFS da un server remoto che potrebbe essere montata senza autenticazione. Per risolverla, configuro NFS in modo che solo host autorizzati possano accedere.

Per modificare le autorizzazioni NFS ho aperto il file export con il comando "sudo nano /etc/exports" ed ho definito le condivisioni NFS.

CRITICAL

NFS Exported Share Information Disclosure

< >

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.

Output

The following NFS shares could be mounted :

+ / Contents of / :
- .
- .
- bin
- boot
MORE...

To see debug logs, please visit individual host

Port

Hosts

2049 / udp / rpc-nfs

192.168.50.101

Plugin Details

Severity: Critical

ID: 11356

Version: 1.21

Type: remote

Family: RPC

Published: March 12, 2003

Modified: August 30, 2023

VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: Unproven

Age of Vuln: 730 days +

Product Coverage: Low

CVSSv3 Impact Score: 5.9

Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.9

Risk Factor: Critical

Name	Schedule	
scan finale 27.10	On Demand	✓
scan vuln. backdoor	On Demand	✓
scan_progetto 27/10	On Demand	✓
scan.27/10	On Demand	✓
Progetto 28/10	On Demand	✓

Dopo aver apportato ciascuna modifica per affrontare le vulnerabilità individuate, ho eseguito una scansione di sicurezza. In seguito a queste azioni correttive, le vulnerabilità precedentemente rilevate non sono più presenti.

scan finale 27.10

< Back to My Scans

Configure

Audit Trail

Launch

Report

Export

Hosts 1

Vulnerabilities 54

Remediations 2

History 1

Filter

Search Vulnerabilities

54 Vulnerabilities

Sev	CVSS	VPR	Nam...	Family	Count	
CRITICAL	10.0		U...	General	1	
CRITICAL	SSGain a shell remotely		3	
MIXED	SSService detection		3	
HIGH	7.5	6.7	S...	General	1	
MIXED	SSGeneral		28	
MIXED	ISDNS		5	
MEDIUM	6.5		T...	Se Plugin ID: 89058	2	
MEDIUM	5.9	4.4	S...	Misc.	1	

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 6:11 PM

End: Today at 6:40 PM

Elapsed: 29 minutes

Vulnerabilities

Critical

High

Medium

Low

Info