

Esercizio: report vulnerabilità

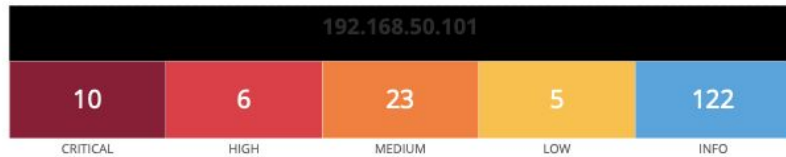
Venerdì 05/08/2022

Ivona Kovacevic

Nessus: Vulnerability Assessment



Abbiamo effettuato una scansione sulle porte del nostro target, ovvero Metasploitable. La funzione adoperata è il “basic network Scan” di Nessus, il quale ha rilevato alcune vulnerabilità.



Scan Information

Start time: Fri Aug 5 03:15:41 2022
End time: Fri Aug 5 03:39:12 2022

Host Information

Netbios Name: METASPLOITABLE
IP: 192.168.50.101
MAC Address: 08:00:27:C6:2E:25
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

- Server scansionato: Metasploitable
- IP server: 192.168.50.101
- **10 critiche** - **6 alte** - **23 medie**

Scansione vulnerabilità: risultato iniziale

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲	Family ▲	Count ▼		
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Export...	RPC	1	🕒	✎
<input type="checkbox"/>	CRITICAL	10.0	Unix Opera...	General	1	🕒	✎
<input type="checkbox"/>	CRITICAL	10.0 *	VNC Server...	Gain a shell remotely	1	🕒	✎
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell ...	Backdoors	1	🕒	✎
<input type="checkbox"/>	CRITICAL	...	2 SSL (...)	Gain a shell remotely	3	🕒	✎
<input type="checkbox"/>	MIXED	...	2 SSL (...)	Service detection	3	🕒	✎
<input type="checkbox"/>	HIGH	7.5	NFS Shares...	RPC	1	🕒	✎
<input type="checkbox"/>	HIGH	7.5	Samba Bad...	General	1	🕒	✎

Notiamo più vulnerabilità sul nostro sistema target ma ci focalizzeremo principalmente su due:

- VNC Server
- Bind Shell Backdoor

61708 - VNC Server 'password' Password

61708 - VNC Server 'password' Password

Synopsis


A VNC server running on the remote host is secured with a weak 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.

La **password** risulta molto debole e per risolvere questa criticità va cambiata, cercando di aumentare il livello di sicurezza.

Esito post-modifica: cambio password

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Exported Share Information Disclosure
<input type="checkbox"/>	CRITICAL	10.0	Unix Operating System Unsupported Version Detection
<input type="checkbox"/>	CRITICAL	9.8	Apache Tomcat AJP Connector Request Injection (Ghostcat)
<input type="checkbox"/>	MIXED	...	 Phpmyadmin (Multiple Issues)

Nella seconda scansione, qui di fianco, possiamo vedere che una volta cambiata la psw, non ci rivela più la criticità.

```
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# cd .vnc
root@metasploitable:/home/msfadmin/.vnc# ls
metasploitable:1.log  metasploitable:1.pid  passwd  xstartup
root@metasploitable:/home/msfadmin/.vnc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin/.vnc#
```

Utilizzando i comandi del prompt su Metasploitable abbiamo modificato la password e l'abbiamo resa più sicura.

51988 - Bind Shell Backdoor Detection

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

Bind Shell Backdoor: una shell sta in ascolto su una porta remota senza che gli venga richiesta l'autenticazione.

Sinossi: l'host remoto è stato forse compromesso

Soluzione: Verificare se l'host sia stato compromesso e aggiungere un firewall.

Esito post-modifica: abilitazione firewall

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲	Family ▲
<input type="checkbox"/>	CRITICAL	10.0 *	Debian Op...	Gain a shell remotely
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Export...	RPC
<input type="checkbox"/>	CRITICAL	10.0	Unix Opera...	General
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell ...	Backdoors
<input type="checkbox"/>	HIGH	7.5	NFS Shares...	RPC
<input type="checkbox"/>	HIGH	7.5	Samba Bad...	General

Dopo aver abilitato il firewall sulla porta della backdoor nella seconda scansione scompare la vulnerabilità “Bind Shell Backdoor Detection”.

```
root@metasploitable:/home/msfadmin# ufw

Usage: ufw COMMAND

Commands:
  enable                Enables the firewall
  disable               Disables the firewall
  default ARG           set default policy to ALLOW or DENY
  logging ARG           set logging to ON or OFF
  allow|deny RULE       allow or deny RULE
  delete allow|deny RULE delete the allow/deny RULE
  status                show firewall status
  version               display version information

root@metasploitable:/home/msfadmin# ufw disable
Firewall stopped and disabled on system startup
root@metasploitable:/home/msfadmin# ufw enable 1524
Firewall started and enabled on system startup
root@metasploitable:/home/msfadmin# ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/home/msfadmin# ufw deny 1524
Rules updated
root@metasploitable:/home/msfadmin# _
```

11356 - NFS exported Share Information Disclosure

Il **protocollo NFS** (network file system) permette al computer client di utilizzare la rete per accedere a directory condivise da server remoti come se fossero disponibili sulla propria rete locale.

Sinossi: E' possibile avere accesso ai NFS shares sul host remoto.

Soluzione: Configurare il NFS sul host remoto cosicché solo gli host autorizzati possano accedervi.

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