Progetto settimanale

vulnerability scanner: NESSUS
target : metasplotable
ip: 192.168.50.101

Vulnerabilità critiche trovate

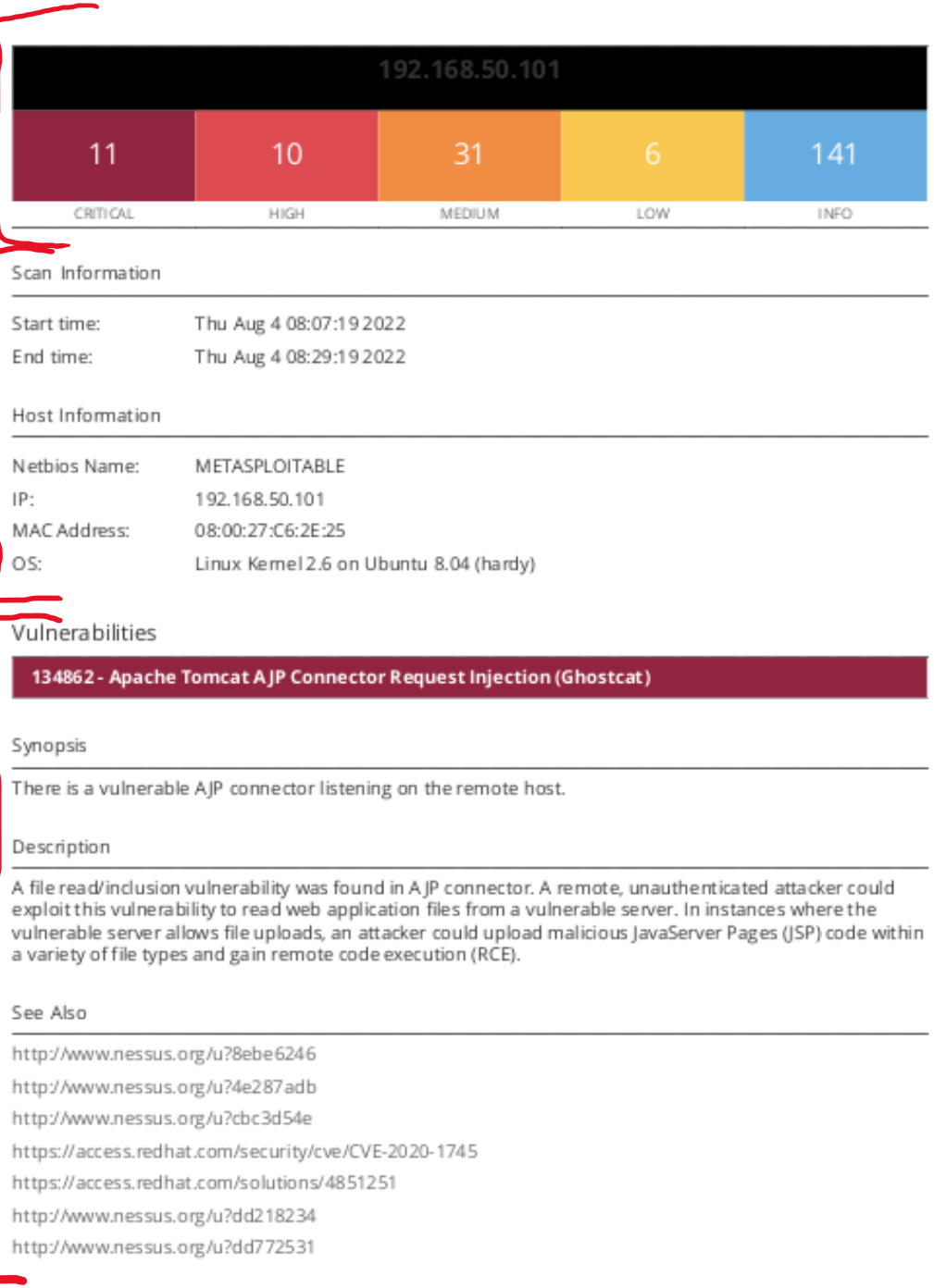
Sev	Score	Name	Family	Count
CRITICAL	10.0 *	NFS Export...	RPC	1
CRITICAL	10.0	Unix Opera...	General	1
CRITICAL	10.0 *	VNC Server...	Gain a shell remotely	1
CRITICAL	9.8	Apache To...	Web Servers	1
CRITICAL	9.8	Bind Shell ...	Backdoors	1
CRITICAL	...	2 SSL (...	Gain a shell remotely	3

Vulnerability assessment

Per quanto rigurda il report ,la prima informazione contenuta nel report è una vista delle vulnerabilità trovate divise in diversi colori

Il blocco successivo contiene delle informazioni generali

In questa parte inizia la sezione di dettaglio di tutte le vulnerabilità
Qui ci indica il nome delle vulnerabilità, una descrizione dettagliata e link correlati



192.168.50.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
11	10	31	6	141

Scan Information

Start time: Thu Aug 4 08:07:19 2022
End time: Thu Aug 4 08:29:19 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)

Vulnerabilities

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis

There is a vulnerable AJP connector listening on the remote host.

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

See Also

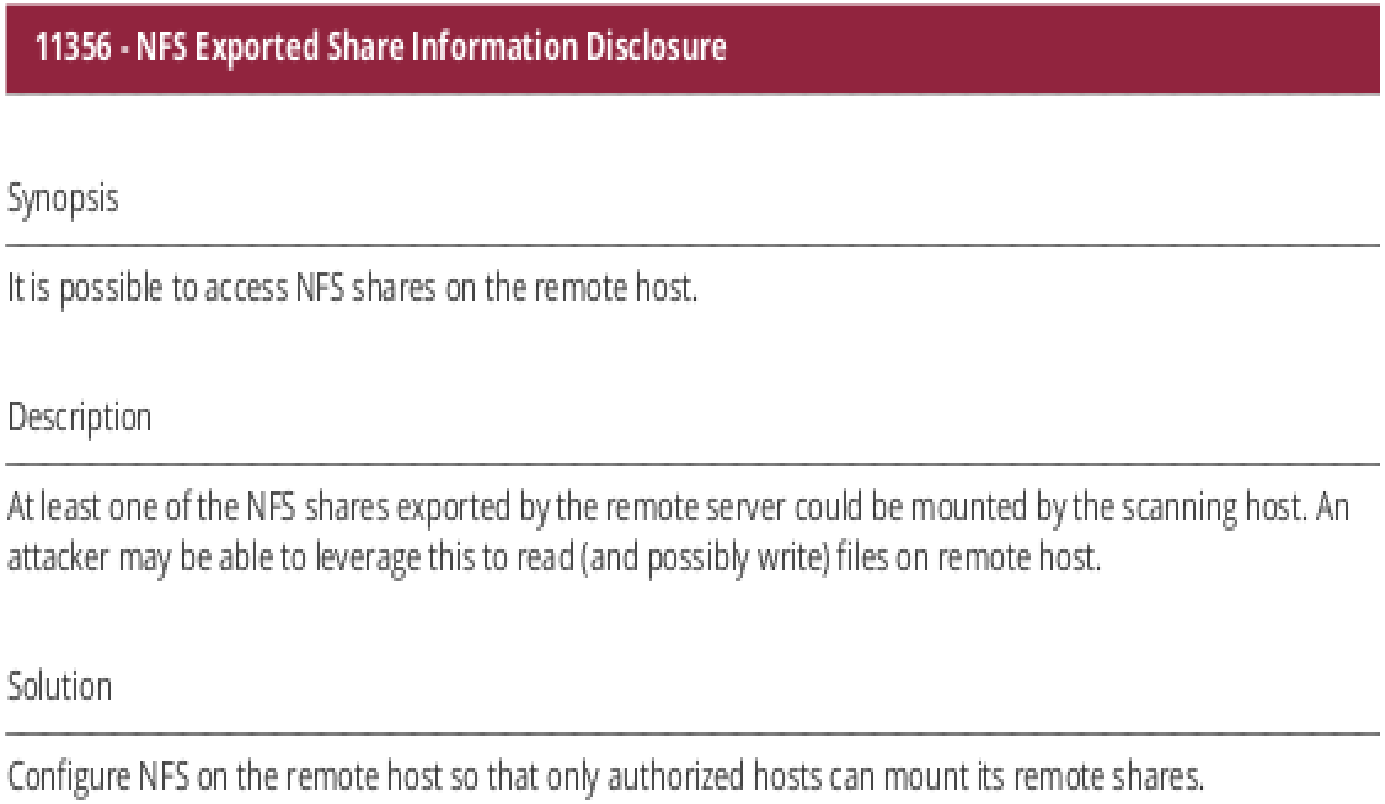
http://www.nessus.org/u?8ebe6246
http://www.nessus.org/u?4e287adb
http://www.nessus.org/u?cbc3d54e
https://access.redhat.com/security/cve/CVE-2020-1745
https://access.redhat.com/solutions/4851251
http://www.nessus.org/u?dd218234
http://www.nessus.org/u?dd772531

11356 - NFS Exported Share Information Disclosure

Sinossi
È possibile accedere alle condivisioni NFS sull'host remoto.

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

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



61708 - VNC Server 'password' Password

Sinossi
Un server VNC in esecuzione sull'host remoto è protetto con una password debole.

Descrizione
Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di 'password'. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questo per prendere il controllo del sistema.

Soluzione
Proteggi il servizio VNC con una password complessa.

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Synopsis

The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote sessior or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Azione di rimedio sulla vulnerabilta61708 - VNC Server 'password' Password

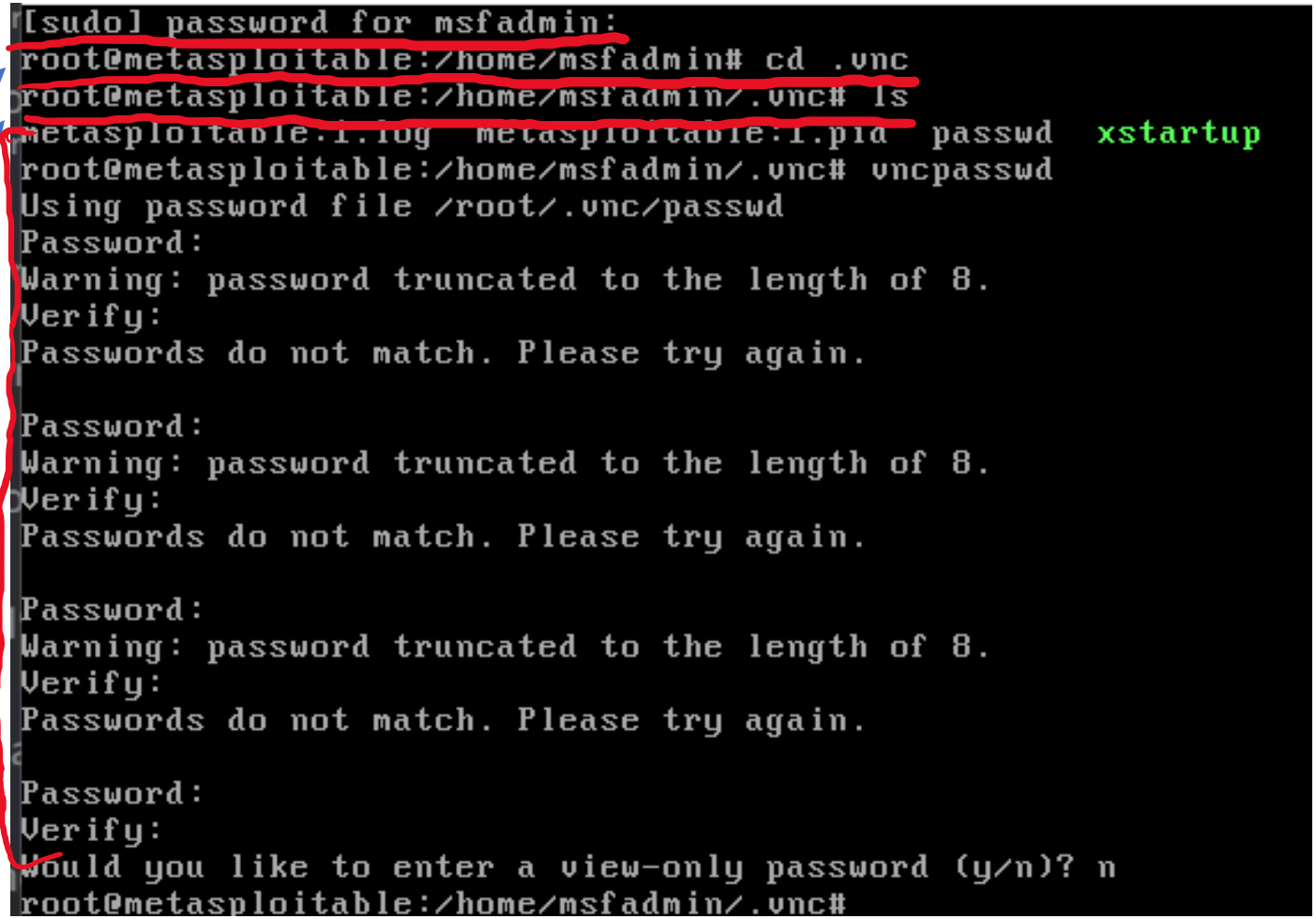
Per eseguire l'azione di rimedio entriamo nella macchina metasploitable , attiviamo la modalita root inserendo la password di default (msfadmin) .

- Inseriamo il codice " cd .vnc" per entrare dentro la directory vnc

-una volta dentro la directory vnc con il comando "ls" vediamo i file al suo interno

-di seguito inseriamo il comando "vncpasswd" per cambiare la password con una più complessa rispettando una lunghezza di non piu 8 caratteri

-poi facciamo il reboot della macchina mataspoitable



51988 - Bind Shell Backdoor Detection

Sinossi

L'host remoto potrebbe essere stato compromesso.

Descrizione

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo da connessione alla porta remota e invio diretto di comandi.

Soluzione

Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

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

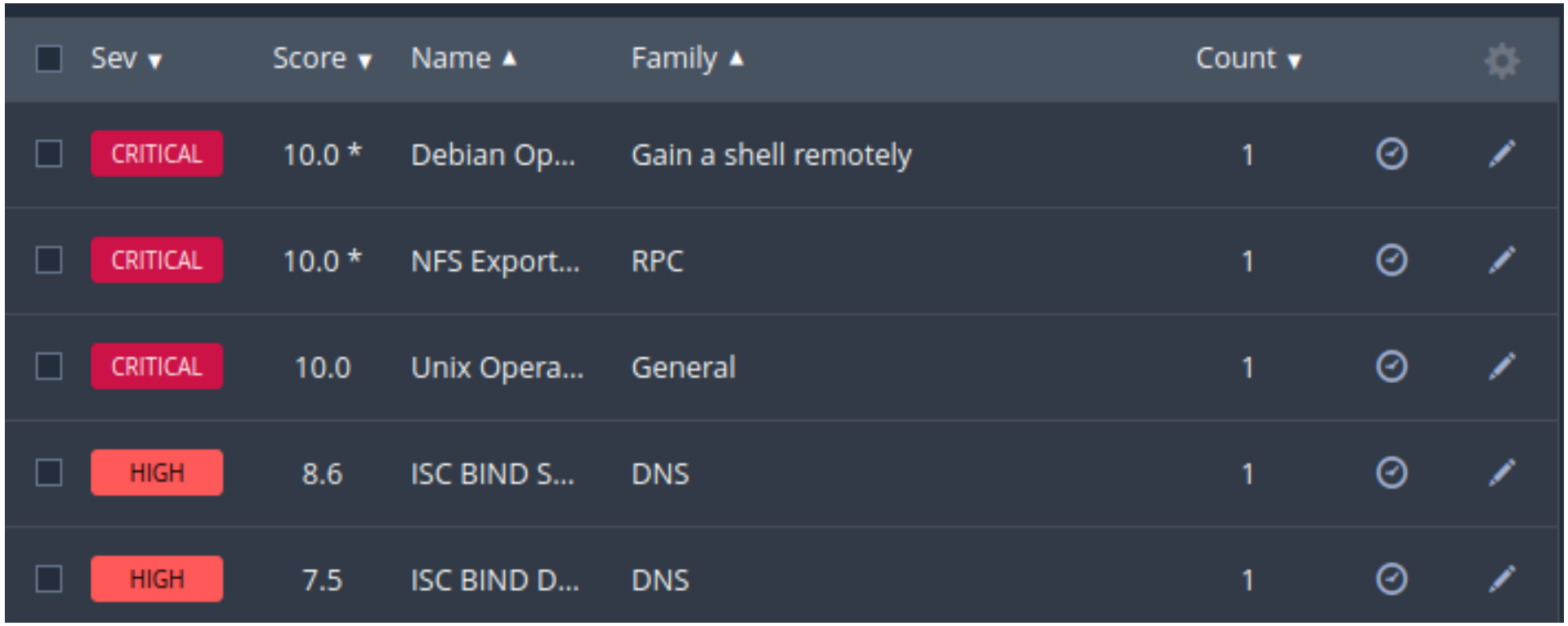
Azione di rimedio sulla vulnerabilta 51988 - Bind Shell Backdoor Detection

Per quanto riguarda il rimedio della bind shell dobbiamo attivare il firewall relativo alla porta interessata in questo caso la p-1524
Di seguito i passaggi sulla macchina metasploit

```
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# _
```

Vulnerabilità trovate dopo aver eseguito vari rimedi

come possiamo notare non si visualizzano più alcune vulnerabilità critiche



Sev	Score	Name	Family	Count
CRITICAL	10.0 *	Debian Op...	Gain a shell remotely	1
CRITICAL	10.0 *	NFS Export...	RPC	1
CRITICAL	10.0	Unix Opera...	General	1
HIGH	8.6	ISC BIND S...	DNS	1
HIGH	7.5	ISC BIND D...	DNS	1