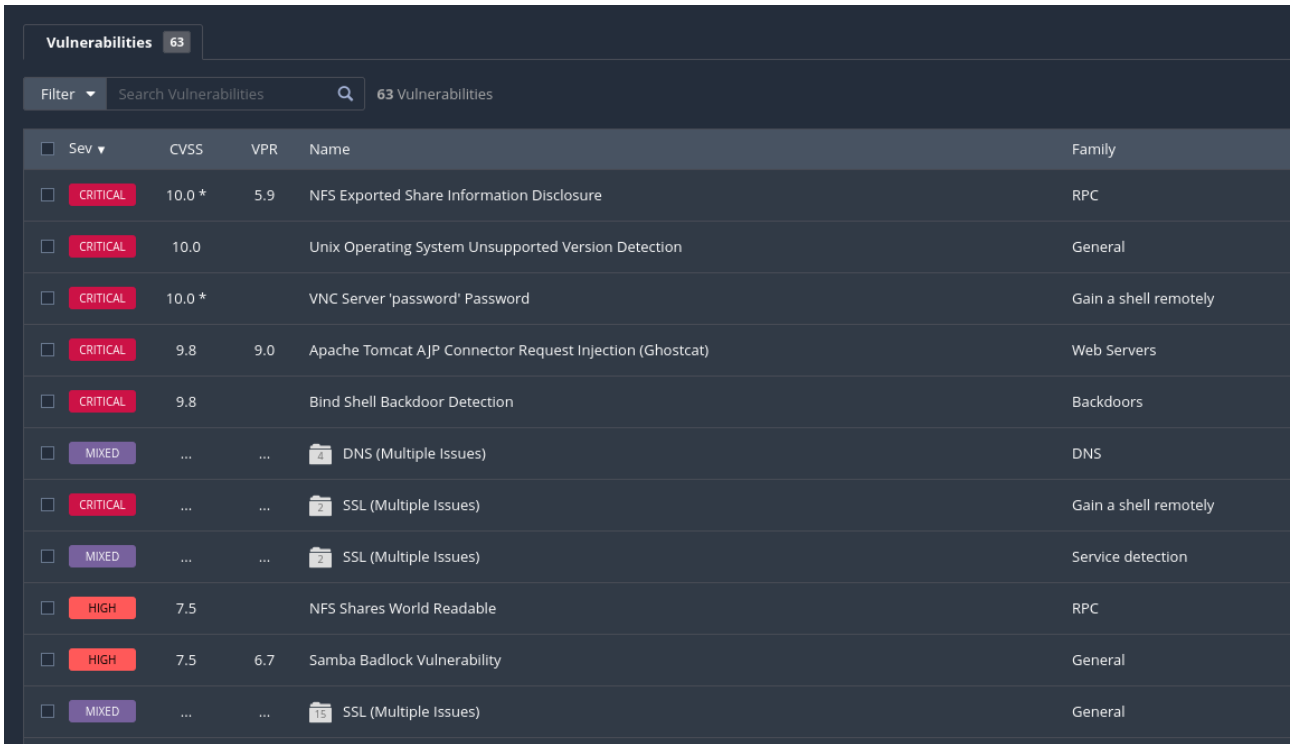
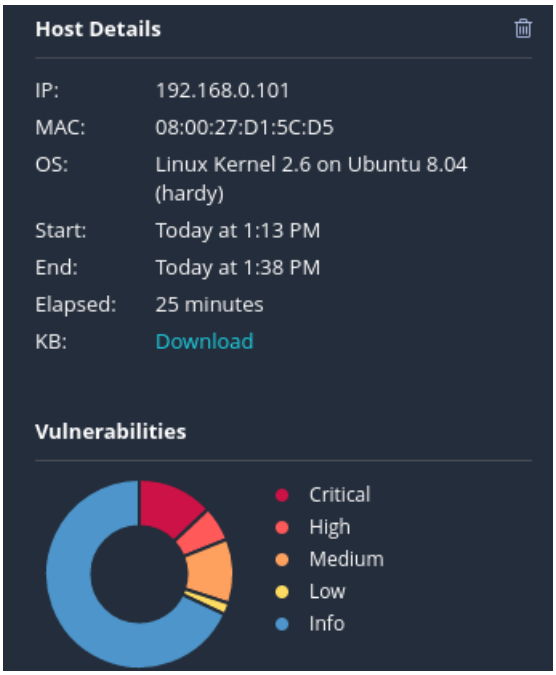
Nell'esercizio di oggi abbiamo eseguito una scansione dell'IP di Metasploitable usando il vulnerability scanner Nessus.



Vediamo che Nessus ha rilevato 63 vulnerabilità in Metasplitable, alcune non gravi (il 66%) altre di gravità crescente da media a critica.



Nessus può generare report più o meno dettagliati delle vulnerabilità riscontrate.

Prendiamo ad esempio il report meno dettagliato.

192.168.0.101

9	4	17	6	74
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 110

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure

Le criticità più pericolose sono quelle con il numero CVSS più alto (vediamo che ne abbiamo 4 a livello 10.0).

La prima vulnerabilità che incontriamo riguarda NFS Share, un protocollo che gestisce lo stoccaggio e il recupero di dati da pate di dispositivi di storage su rete (in pratica un fyle system di rete).

CRITICAL **NFS Exported Share Information Disclosure**

Description

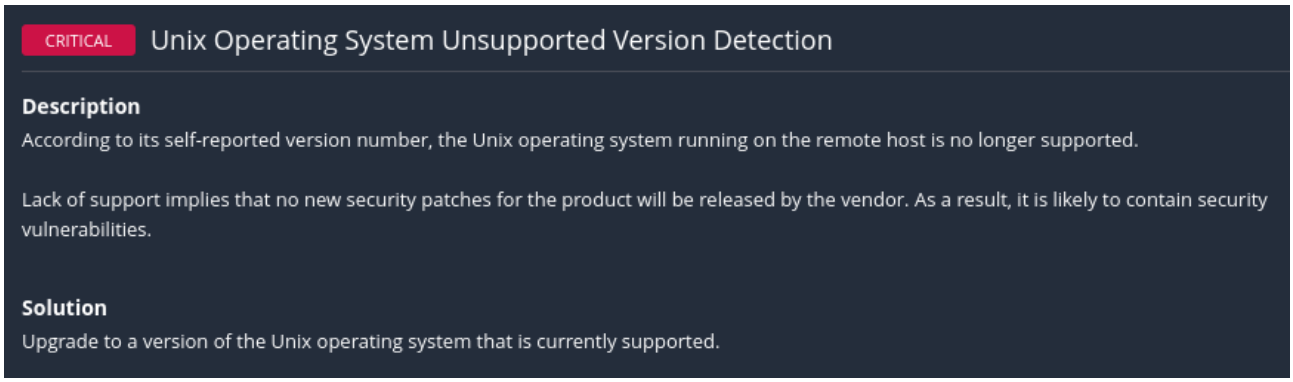
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

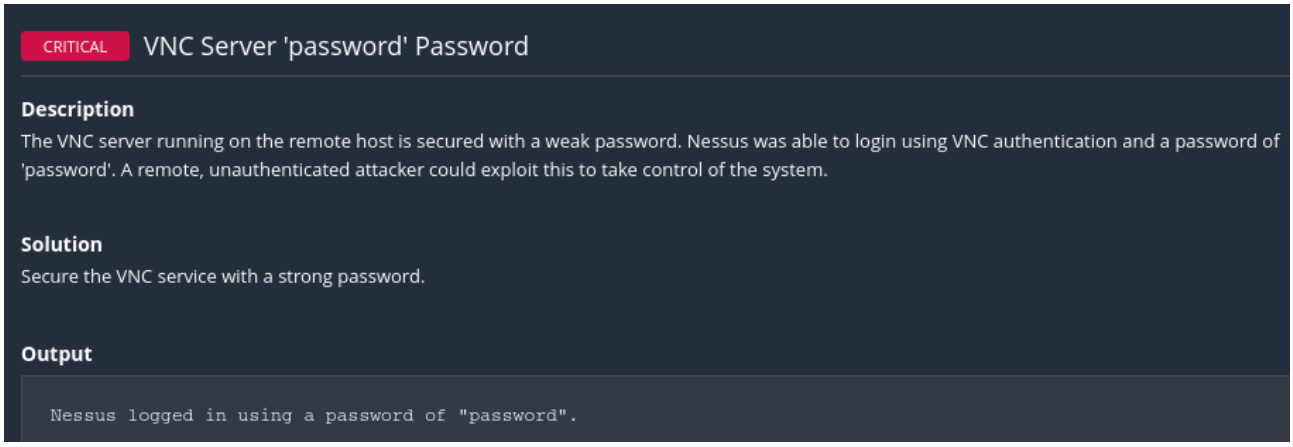
Nessus ci informa che almeno uno degli NFS può essere attaccato e i file in esso contenuti letti o persino riscritti.
La soluzione che ci viene proposta è di mettere al sicuro gli NFS configurando una regola che permetta solo a determinati host di accedervi (potrebbe essere fatto tramite una regola di firewall).

La seconda vulnerabilità è piuttosto comune e riguarda l'intero sistema operativo.



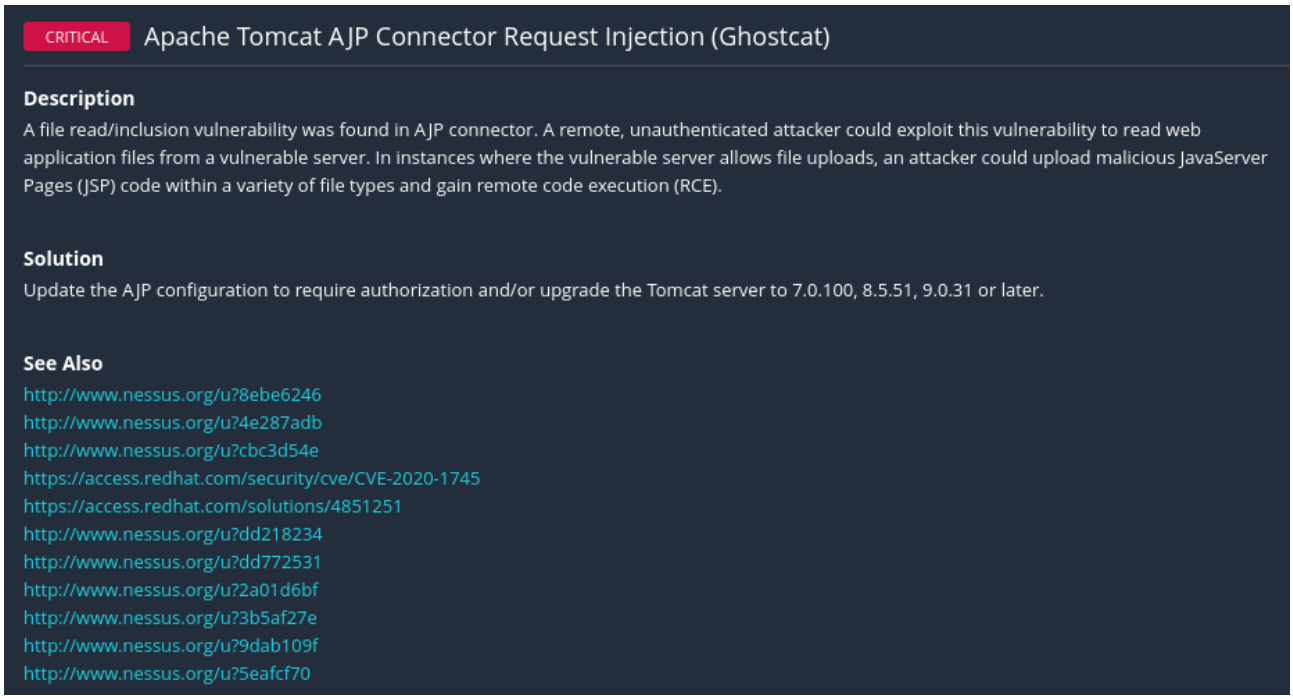
La versione del sistema operativo è obsoleta e non è più supportata (di conseguenza no vengono più rilasciate patch per risolvere errori e vulnerabilità). La soluzione più ovvia è quella di fare l'upgrade ad una versione del sistema operativo più recente e supportata.

La terza vulnerabilità è un'altra di quelle più comuni, cioè la sicurezza della password.



La password settata è proprio “password”, una delle parole chiave più vulnerabili; è una situazione molto facilmente sfruttabile da un black hat e l'unica soluzione possibile è impostare una password più forte, fatta di almeno 8 caratteri (possibilimente di più) e composta da lettere minuscole, maiuscole, numeri e caratteri speciali.

Infine abbiamo una vulnerabilità riscontrata sul web server, sul protocollo AJP.



Un attaccante potrebbe sfruttare questa vulnerabilità per accedere a file presenti nel web server o persino caricare malware (o file contenenti malware) nel server stesso.
In questo caso Nessus ci propone due soluzioni: cambiare la configurazione del protocollo AJP in modo che sia necessaria un'autorizzazione per accedere al server o aggiornare ad una versione più recente il server stesso.