S5L5 - Progetto | Scansione completa di Metasploitable

Gruppo: **NetRaiders**
Matteo Leoni, Rosario Giaimo, Claudio Maida,
Gianmarco Mazzoni, Lorenzo Moro, Stefano Di Prospero.

Consegna:

Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio.
N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili.
Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità.
Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Vulnerabilità critiche trovate con la prima scansione:
8 **critiche**, 4 alte, 16 medie, 6 basse.

Analizziamo e risolviamo le più critiche.

Bind Shell Backdoor Detection:

Attraverso l'utilizzo di iptable sulla macchina Metasploitable siamo riusciti a filtrare la porta interessata, **`1524`**, droppando tutte le connessioni in ingresso su quella porta.
N.B.: Se questa configurazione di iptables viene salvata, ma non su rc.local con iptables-restore, è necessario modificarla nuovamente una volta riavviata, perché le impostazioni non vengono mantenute. Quindi, per prevenire abbiamo modificato direttamente il file "**`rc.local`**" aggiungendo **`iptables-restore`** all'interno del file.

VNC Server 'password' Password:

Per risolvere questo problema, abbiamo modificato la password indicata, tramite i comandi:
`sudo su`
Per ottenere privilegi di root
`vncpasswd`
Scegliendo una password leggermente più complessa, è possibile risolvere questa falla di sicurezza.

Apache Tomcat AJP Connector Request Injection (Ghostcat)

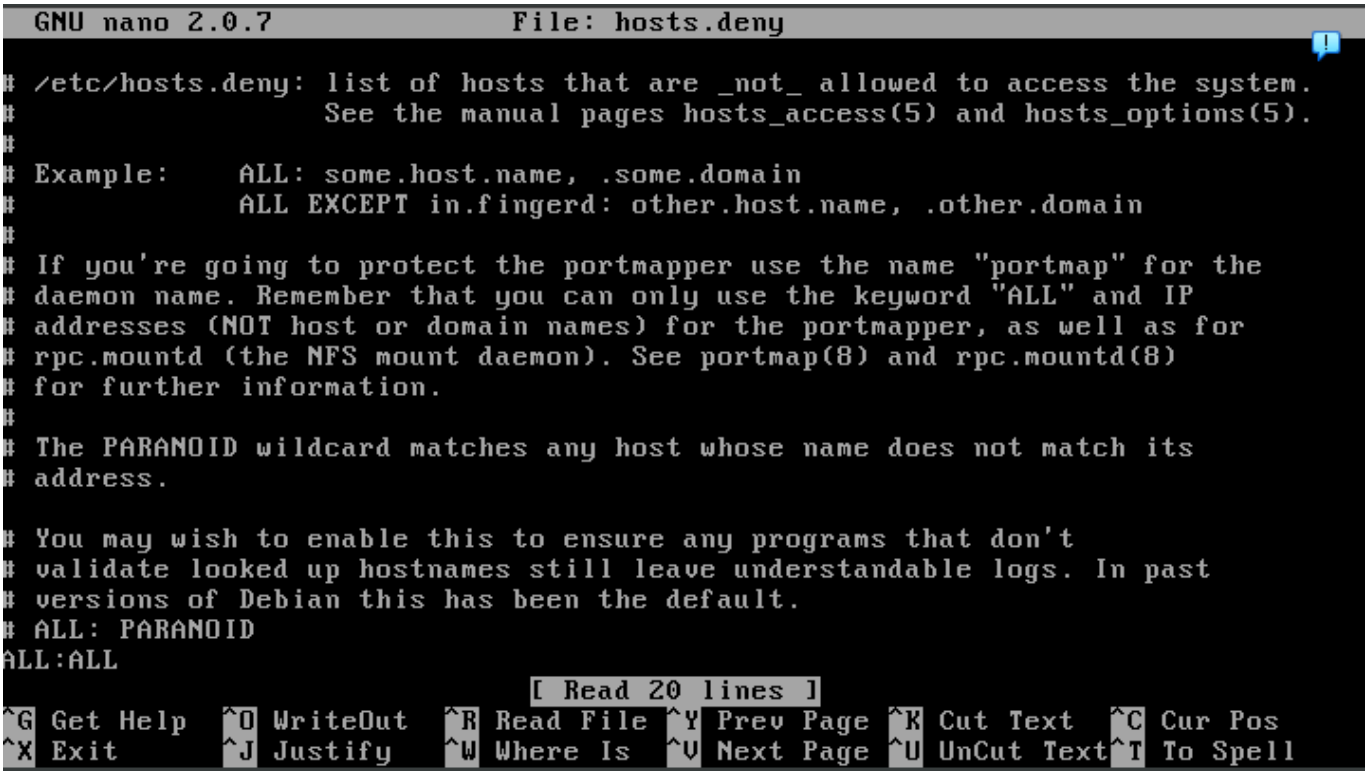
Questa vulnerabilità può causare molteplici rischi di sicurezza, quali RCE e Denial of Service.
È stata risolta disabilitando il servizio AJP Connector **`apache2`**.

NFS Exported Share Information Disclosure

Questa falla permette l'accesso a dispositivi non autorizzati a dati sensibili:

Configurazione **`~/etc/hosts.allow`**

Configurazione **`~/etc/hosts.deny`**



Con **`ALL:ALL`** vengono negate in entrata tutte le connessioni non indicate nel file allow, quindi fa eccezione di **`192.168.50.101`**.

Conseguentemente alle modifiche effettuate, dopo una seconda scansione del sistema Metasploitable, abbiamo notato che sono state risolte ulteriori criticità rilevate precedentemente.

Vulnerabilità critiche trovate con la seconda scansione, dopo le nostre modifiche:
2 **critiche**, 3 alte, 14 medie, 3 basse, si è eseguita quindi una riduzione di 12 vulnerabilità.

Vengono allegati i report effettuati, che saranno anche disponibili nella repository di GitHub.