

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`

```
GNU nano 2.0.7 File: hosts.allow

# /etc/hosts.allow: list of hosts that are allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: LOCAL @some_netgroup
#              ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
sshd: 192.168.50.101

[ Read 14 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

Configurazione `~/etc/hosts.deny`

```
GNU nano 2.0.7 File: hosts.deny

# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: some.host.name, .some.domain
#              ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
ALL:ALL

[ Read 20 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

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.