

PROGETTO GIORNO 5

Per questo progetto abbiamo dovuto fare una scansione completa di Nessus sulla nostra macchina virtuale Metasploitable.

Da Nessus abbiamo scaricato il report completo delle vulnerabilità della nostra macchina, esportandone quelle critiche ed evidenziando quelle da risolvere.



192.168.32.101



Vulnerabilities

Total: 134

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	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	9.8	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	61708	VNC Server 'password' Password

Scegliere da 2 a 4 vulnerabilità critiche sulla macchina Metasploitable2 per poi provare ad implementare delle azioni di rimedio.

Abbiamo evidenziato le vulnerabilità critiche da risolvere.

Per dimostrare l'efficacia delle azioni di rimedio eseguire nuovamente la scansione sul target e confrontare i risultati con quelli precedentemente ottenuti.

Remediation:

- **VNC Server 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 sfruttarlo per assumere il controllo del sistema.

Soluzione:

Proteggi il servizio VNC con una password complessa.

Fattore di rischio:

Critico

Host:

192.168.32.101

Porta:

TCP/5900/VNC

Nessus ha effettuato l'accesso utilizzando una password di "password".

Andremo quindi a cambiare la password di VNC tramite i passaggi in figura:

```
root@metasploitable:~# /etc/init.d/networking restart
* Reconfiguring network interfaces... [ OK ]
root@metasploitable:~# ls -la
.                  .config           .gconf             .profile           .ssh
..                 Desktop           .gconfd            .purple            .vnc
.bash_history      .filezilla        .gstreamer-0.10    reset_logs.sh      vnc.log
.bashrc            .fluxbox          .mozilla           .rhosts            .Xauthority
root@metasploitable:~# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~#
```

- **Rilevamento backdoor Bind Shell**

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 connettendosi alla porta remota e inviando direttamente comandi.

Soluzione:

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

Fattore di rischio:

Critico

Porta:

TCP/1524/wild_shell

Nessus è stato in grado di eseguire il comando "id" utilizzando la seguente richiesta:

Ciò ha prodotto il seguente output troncato (limitato a 10 linee):

```
root@metasploitable:~# uid=0(root) gid=0(root) groups=0(root)
```

root@metasploitable:/#

Andremo ad aggiungere un FireWall sulla porta 1524 tramite i comandi:

```
[sudo] password for msfadmin:
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#
```

Per fare un controllo, andremo a lanciare una scansione con nmap sulla macchina Kali per confermare che la porta in questione, la 1524, risulterà filtrata.

```
(kali@kali)-[~]
$ nmap 192.168.32.101 -sT
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-25 11:18 EST
Nmap scan report for 192.168.32.101
Host is up (0.00060s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.45 seconds

(kali@kali)-[~]
$
```

- **Divulgazione di informazioni sulle azioni esportate NFS**

Sinossi:

È possibile accedere alle condivisioni NFS sull'host remoto.

Descrizione:

Almeno una delle condivisioni NFS esportate dal server remoto può essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file su host remoto.

Soluzione:

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

Fattore di rischio:

Critico

Porta:

UDP/2049/RPC-NFS

Andremo a risolvere tramite:

```

GNU nano 2.0.7      File: exports
# /etc/exports: the access control list for filesystems which may be exported
#                 to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
/mnt/newdisk      192.168.32.101(rw,sync,no_root_squash,no_subtree_check)

[ Wrote 12 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   ^U Next Page  ^U UnCut Text ^T To Spell

```

Riproveremo quindi una scansione con Nessus sulla macchina Metasploitable2:

192.168.32.101



Vulnerabilities Total: 128

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Com'è possibile vedere dalla nuova scansione di Nessus le vulnerabilità critiche evidenziate sono state risolte.