Advies rapport

Linux server

Project	Testrapport
Opdrachtgever	Fysio-bakker
Auteur(s)	……
Datum	……
Versie	…….

Limaweg 25 | 2743 CB | Waddinxveen
+31 (0)172 211 120
info@worldskillsnetherlands.nl
worldskillsnetherlands.nl

Advies rapport Linux server

Inleiding

Dit rapport beschrijft het test en advies rapport en de instellingen van de firewall van de Linux server.

Firewall

Voor het beveiligen van de server dienen de onderstaande regels in de firewall (iptables) toegevoegd te worden aan de server.

*** Blokkeer ssh wanneer er meer dan acht sessies binnen 45 seconden geopend worden.**

iptables -A INPUT -p tcp --dport ssh -m conntrack --ctstate NEW -m recent --update --seconds 45 --hitcount 8 -j DROP

*** Alleen jullie laptops krijgen toegang tot de server (schrijf hiervoor één regel)**

iptables -I INPUT -p tcp -s 172.16.0.X, 172.16.0.X1 --dport ssh -j ACCEPT

iptables -I INPUT -p tcp --dport ssh -j DROP

*** Beveilig de server voor port scanning**

iptables -N PORT-PROTECT

iptables -A PORT-PROTECT -p tcp --syn -m limit --limit 2000/

hour -j RETURN

iptables -A PORT-PROTECT -m limit --limit 200/hour -j LOG

--log-prefix "DROPPED Port scan: "

iptables -A PORT-PROTECT -j DROP

iptables -A INPUT -p tcp --syn -j PORT-PROTECT

Test en aanbeveling Linux server

Beschrijf in onderstaande tabel in de kolom hoe je de test hebt uitgevoerd, in de kolom risico beschrijf je het riscio en in de kolom schrijf de aanbeveling.

item	test	risico	aanbeveling
Laatste upgrade is uitgevoerd?	skill@linxhard:~$ cat /var/log/apt/history.log | grep End-Date End-Date: 2023-03-08 09:53:16	Het systeen kan niet gepachte vulnerabilities hebben.	Periodiek het systeem updaten en upgraden.
Laatste update is uitgevoerd?			
Home is geencrypt op een eigen volume?	Command0: blkid TYPE="ext4" Het volume is niet geencrypt	De schijf kan gelezen worden zonder in ingeloged te zijn.	Home dir encrypten.
Systeem ontvangt automatisch updates en installeerd deze?	root@linxhard:/etc/apt/apt.conf.d# systemctl status unattended-upgrades ● unattended-upgrades.service - Unattended Upgrades Shutdown Loaded: loaded (/lib/systemd/system/unattended-upgrades.service; enabled; vendor preset: enabled) Active: active (running) since Wed 2023-03-08 09:47:17 UTC; 25min ago Docs: man:unattended-upgrade(8) Main PID: 672 (unattended-upgr) Tasks: 2 (limit: 2238) Memory:	Door de automatische updates kan een update (met fouten) het systeem breken.	In de configuratie van het bestand alleen security updates automatisch installeeren.

	12.1M CPU: 75ms CGroup: /system.slice/unattended-upgrades.service └─672 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal Mar 08 09:47:17 linxhard systemd[1]: Started Unattended Upgrades Shutdown. root@linxhard:/etc/apt/apt.conf.d#		
Lagecy services zijn verwijderd? Rsh, rlogin, rcp, ypserv, ypbind, tftp, talk	Sudo apt remove “service naam” Alle services zijn verwijderd	Oude services kunnen vunrabilities hebben.	On nodige en oude services verwijderen.
Services die niet gebruikt worden zijn uitgeschakeld? vb. FTP, DNS, LDAP, SMB, DHCP, NFS SNMP	Sudo systemctl status “service naam” Alle services zijn uitgeschakeld.	Services die niet gebruikt worden kunnen vunrabilities hebben die gebruikt kunnen worden om toegang te krijgen tot de server.	Alle nietgebruikte services uitschakelen.
NTP is ingeschakeld?	Comando: ntpq is niet inegschakkeld.	De datum en tijd kan niet goed lopen. Hierdoor kunnen log bestanden een verkeerde tijd en datum aangeven.	NTP inschakkelen .
Controleer de volgende instellingen: SSH protocol:	Cat /etc/ssh/sshd_config	SSH 1 gebruikt een andere (slechtere) manier van encripty waardoor het	Het is te adviseren deze instellingen in te stellen.

version 2 log leve is set to INFO PermitemptyPassword is set to No	SSH versie 2 Log staat op INFO Permitemptypassword is no	systeem vunrable word. Zonder logs word het moeilijk om een hacker zijn aanval te onderzoeken. Inloggen zonder wachtwoord is niet toegestaan.	
Root login account is over SSH gedisabeld?	nano /etc/ssh/sshd_config #PermitRootLogin prohibit-password	Het root account is dan vunrable voor een bruteforce attack.	Root over ssh uitschakellen.
Account hebben een veilig wachtwoord van minimaal 12 karakters?	nano /etc/pam.d/common-password	Korte en slechte wachtwoorden kunnen makkelijk geraden worden met een bruteforce attack.	Wachtwoord policies instellen.