Készítette: Babusa Tamás

adatok:

deb 10 lts

user, pass

openssh

192.168.0.37

hardening:

backup mindenről

sudo

ssh

echo '

PasswordAuthentication no

PermitRootLogin no

AddressFamily inet

Port 2222

' | sudo tee -a /etc/ssh/sshd\_config

nftables

chain input {

# accept any localhost traffic

# accept traffic originated from us

# drop invalid packets

ct state invalid counter log prefix "riasztas" drop

# accept ssh, http, and https

# accept icmp

# count and reject everything else

chain forward {

type filter hook forward priority 0; policy drop;

}

chain output {

type filter hook output priority 0; policy accept;

}

apps:

ntp

apache2 - http

<VirtualHost \*:80>

sudo chown -R www-data:www-data /var/www/html/dwsbt.site/public\_html

sudo chmod -R 755 /var/www/html/dwsbt.site/public\_html

sudo a2ensite dwsbt.site

sudo a2dissite 000-default.conf

A vállalatunk HTTP szolgáltatását Linux kiszolgálóra telepítettem. Kiszolgálónak egy virtuális számítógépet használtam, Debian 10 LTS operációs rendszerrel. A szolgáltatáson kívül több egyéb alkalmazás is beállításra került, ami elsősorban a biztonságot és kismértékben a kényelmet szolgálja. Az így felépített webszerver a helyi hálózat és az internet felől is elérhető. A külső elérést a határ routeren beállított port forwarding biztosítja. Ezen kívül az SSH is működik külső hálózatból, szintén Ford port forwarding segítségével.

Hardening:

Az összes módosított konfigurációs fájlról másolatot készítettem, így sokkal könnyebbé válik az esetlegesa visszaállítás.

A root felhasználót letiltottam biztonsági okokból. Helyette egy sudoer felhasználóval lehet dolgozni. Az SSH beállításánál egy biztonságos hosszúságú SHA kulcsot használok. Password helyett passphrase-t használok. Jelszóval nem lehetséges bejelentkezni. Root felhasználóval sem lehet be SSH-zni. Továbbá letiltottam az IPv6-os címeket. Az alapértelmezett 22-es portját 2222 lecseréltem.

A kissé nehézkes IP tables tűzfal alkalmazást töröltem, helyette NF tables-t használok. Alapvető filozófiám volt, hogy csak és kizárólag azt engedem át a tűzfalon, ami a minimális működéshez szükséges. Az illegális csomagokat automatikusan kiszűri és a megfelelő .log fájlba elkönyveli ennek tényét. Fogadja az SSH, HTTP és a z ICMP csomagokat, minden más próbálkozást megszámol és logol. A forwarding tiltva van és a kifelé irányuló adatforgalom teljes egészében engedélyezett.

Szolgáltatások:

A HTTP szolgáltatáson kívül egy NTP-t is telepítettem az online időszinkronizálás miatt. http-nek az Apache2-t választottam. Praktikus okokból a nyolcvanas, alapértelmezett portot hagytam meg a weblap eléréséhez. A weblap elérére a www-Data user jogosult, ezért ennek elérési jogait korlátoztam olvasásra és végrehajtásra a weblap mappájában. Az alapértelmezett WWW mappát letiltottam. Ezzel a weblap illetéktelenek számára nem módosíthatóvá vált. mivel a weblapunk statikus, erre nincs is szükség.

Tesztelés:

A tesztelést két részre bontottam; először a hardeninget, utána magát a HTTP szolgáltatást teszteltem.

A hardening tesztelésénél megpróbáltam be SSH-zni mind helyi, mind távoli hálózatról. Root felhasználóval nem jártam sikerrel. A jelszó használata nem megengedett. Nem lehet bejelentkezni IPv6-os címen sem, mivel nincs ilyen. Nem elérhető a szerver, ha SSH-nál Nem adjuk meg ha 2222-es portot. Az alapértelmezett 22-es szintén nem elérhető

A szerver megfelelő .log fájljait átnézve találtam riasztásokat.

Próbaképpen letiltottam az ICMP, SSH és a http protokollokt és megpróbáltam elérni ezeket a szolgáltatásokat. Ezek természetesen tiltott állapotban nem működtek. Ezt követően a szerverről próbáltam megpingelni különböző helyi és távoli hálózatok hosztjait. Ezek az elvárásoknak megfelelően működtek. A HTTP szolgáltatás bármely hálózatban működött, visszaadta a feltöltött weblapunkat.

A Debian szerver működőképes, megfelelően konfigurált a projekt többi részéhez, és kellő védelemmel van felvértezve, így el tudja látni a delegált funkciókat.