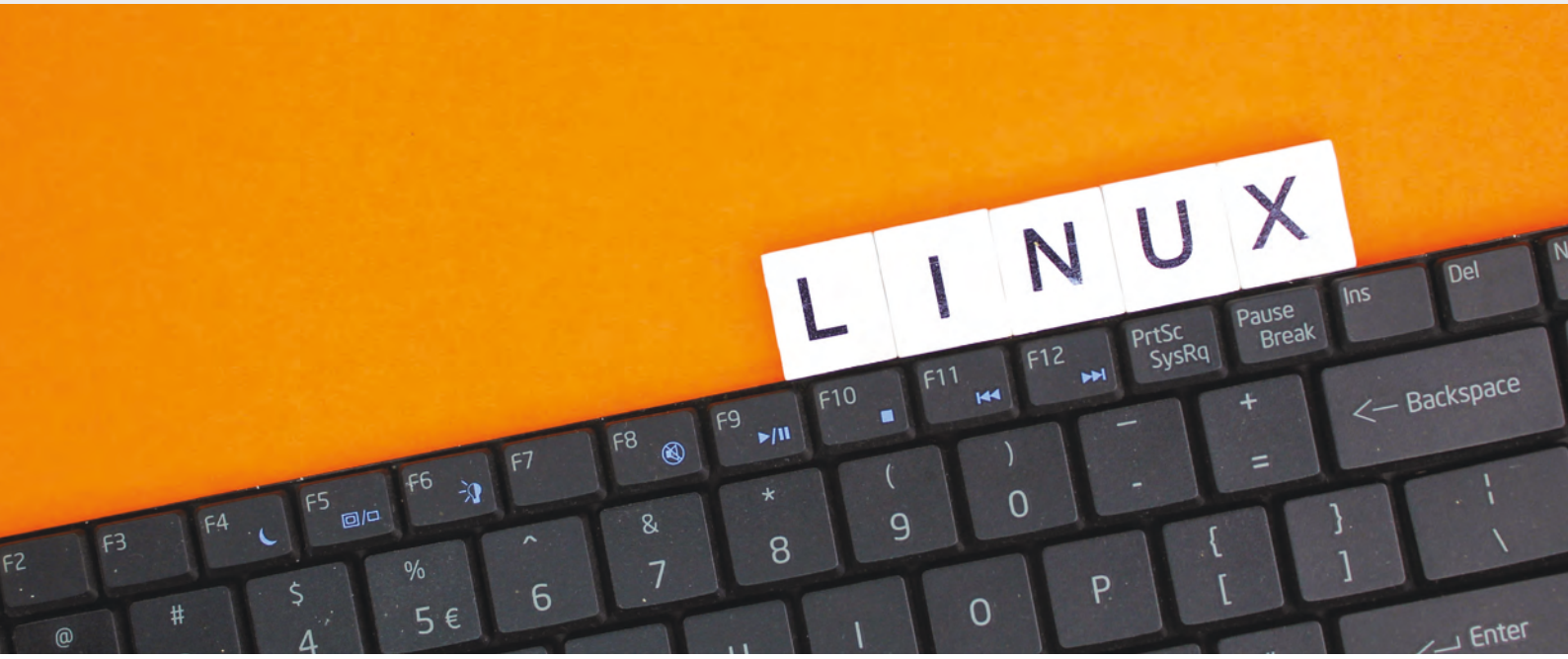
Auteurs: Vincent van Dijk en Chris de Vries. Vincent van Dijk is eigenaar van Security Scientist en is bereikbaar via vincent@securityscientist.net. Chris de Vries is redacteur van het IB Magazine en daarnaast eigenaar van De Vries *Impuls* Management, hij is bereikbaar via impuls@euronet.nl.



Ook Linux-systemen niet immuun voor bedreigingen

HULPGIDS BEVEILIGING VOOR HET KLEINBEDRIJF (DEEL 5)

Linux, een krachtige en veelzijdige besturingssysteemfamilie, staat bekend om zijn robuuste beveiligingskenmerken en wordt daarom vaak gebruikt voor serveromgevingen. Echter, ongeacht hoe veilig een systeem is, is het nooit immuun voor alle mogelijke bedreigingen. Beheerders en gebruikers moeten een proactieve rol spelen om hun systemen te beveiligen en te onderhouden, en dat begint met een grondig begrip van het beveiligingslandschap en de beschikbare tools en configuraties.

In dit artikel duiken we in de wereld van Linux-beveiliging, waarbij we diverse aspecten verkennen zoals initiële installatie en configuratie, de configuratie van firewalls en secure shell (SSH), systeemmonitoring, en regelmatige beveiligingsaudits. Dit artikel biedt inzichtelijke informatie en praktische stappen om de beveiliging van Linux-systemen te versterken en optimaliseren.

Net zoals bij de vorige Windows en Mac artikelen zullen we de volgende onderwerpen behandelen.

1. Hygiëne;
2. Veilige configuratie;
3. Systeemkennis.

Hygiëne

Het actueel houden van systeembestanden is een essentieel onderdeel voor het onderhouden van Linux-systemen. Het regelmatig bijwerken van het systeem en de geïnstalleerde softwarepakketten zorgen ervoor dat beveiligingslekken worden verholpen, en dat het systeem is beschermd tegen bekende bedreigingen. Gebruik voor updates (command-line) pakketbeheerders zoals: de Advanced Package Tool (APT) voor Debian-gebaseerde systemen en yum voor Red Hat-gebaseerde systemen. Standaard voert Ubuntu namelijk (Debian-gebaseerde Linux-systeem) geen automatische updates uit. Hiervoor moet je de 'unattended-upgrades' package installeren en configureren.

Het is belangrijk om alleen de noodzakelijke diensten en toepassingen op het systeem te laten draaien. Onnodige diensten kunnen potentiële ingangspunten voor aanvallers zijn en het deactiveren of verwijderen ervan vermindert het aanvalsoppervlakrisico van het systeem. Gebruik daarom de APT of yum commando's om packages te beheren en te installeren waar nodig.

Gebruik je het Linux-systeem ook voor het dagelijks gebruik, zoals browsen, dan is het ook daar goed om je browser goed in te stellen. Browserhygiëne is ook belangrijk, vooral omdat de meeste gebruikers veel tijd online doorbrengen. Regelmatig wissen van browsercache, cookies en geschiedenis kan helpen om persoonlijke informatie te beschermen en blootstelling aan online bedreigingen te verminderen. Het installeren en gebruiken van browserextensies voor beveiliging, zoals uBlock Origin en HTTPS Everywhere, helpen ook bij het verhogen van de onlinebeveiliging.

Veilige configuratie

Het adequaat configureren van firewalls is van essentieel belang om systemen te beschermen tegen ongewenste toegang en aanvallen van buitenaf. Dit vormt de eerste verdedigingslinie tegen kwaadwillende activiteiten. Met behulp van Uncomplicated FireWall (UFW) kunnen gebruikers firewall-regels beheren, waardoor specifieke poorten en diensten toegankelijk worden, terwijl andere worden geblokkeerd. Deze tools zijn cruciaal voor het reguleren van inkomend en uitgaand verkeer op een Linux-systeem. Zeker omdat een Linux-systeem niet standaard met een firewall komt. Daarbovenop is het echt een vereiste om Fail2Ban installeren. Fail2Ban zorgt ervoor dat IP adressen die kwaadwillig aankloppen geblokkeerd worden als ze dat te vaak proberen: oftewel brute force bescherming.

Zeker bij servers wordt er vaak gebruik gemaakt van Secure Shell (SSH). Dat is sleutelgebaseerde authenticatie: een veiliger alternatief voor wachtwoordauthenticatie. Het gebruik van SSH-sleutels minimaliseert het risico op ongeautoriseerde toegang door brute force-aanvallen en andere soorten inbreuken alsook helpt het om de standaard SSH-poort te veranderen naar een ander port-nummer om de meeste geautomatiseerde aanval tools te slim af te zijn. Het uitschakelen van het root-account op Linux kan de beveiliging verhogen, omdat het aanvallers een potentieel doelwit ontneemt.

Hier volgen de stappen om het root-account uit te schakelen en over te stappen naar een gebruikersgebaseerdsysteem:

1. Maak een Sudo-Gebruiker:
Voordat u het root-account uitschakelt, moet u een nieuwe gebruiker aanmaken en deze sudo-rechten geven, zodat u beheerderstaken kunt uitvoeren.

```
sudo adduser <gebruikersnaam>
sudo usermod -aG sudo <gebruikersnaam>
```

Vervang <gebruikersnaam> met de gewenste gebruikersnaam.

2. Login onder de nieuwe gebruikersnaam:
Log uit als root en log vervolgens in met de nieuwe gebruikersaccount.

3. Pas SSH Configuratie aan:
Bewerk de SSH-configuratie om root-login via SSH te verbieden.

```
shell
sudo nano /etc/ssh/sshd_config
```

Zoek naar de regel die PermitRootLogin bevat en wijzig deze naar:

```
shell
PermitRootLogin no
```

Sla de wijzigingen op en herstart de SSH-service:

```
shell
sudo systemctl restart sshd
```

4. Schakel Root-Account Uit:
Nadat u hebt bevestigd dat u kunt inloggen en sudo kunt gebruiken als nieuwe gebruiker, kunt u het root-account uitschakelen door het wachtwoord te

verwijderen:

shell

sudo passwd -l root

Dit commando vergrendelt het root-account door het wachtwoord te verwijderen, zodat niemand ermee kan inloggen.

5. Beheer het Systeem met Sudo:
Nu, in plaats van in te loggen als root, logt u in als normale gebruiker (uw eigen gebruikersaccount) en gebruikt u sudo om commando's uit te voeren die verhoogde rechten vereisen.

Systeemkennis

Om jouw Linux-systeem veilig te houden, is het handig het systeem te bestuderen. Onderzoek hierbij het navolgende:
1. Folder en gebruikersrechten;
2. Netwerkinstellingen, zoals de firewall en
3. Inspectie van de logs.

Folder en gebruikersrechten

Het grondig begrijpen en correct implementeren van folder- en gebruikersrechten is cruciaal voor de beveiliging van Linux-systemen. In Linux worden permissies toegewezen aan bestanden en directories. Deze permissies bepalen wie deze kan lezen, schrijven of uitvoeren en zijn gecategoriseerd voor de eigenaar, de groep waartoe de eigenaar behoort, en alle andere gebruikers. Het is noodzakelijk om begrip te hebben van Read (lezen), Write (schrijven), en Execute (uitvoeren) permissies voor het instellen van adequate toegangscontroles. Commando's zoals chmod worden gebruikt om permissies te wijzigen en chown en chgrp om de eigenaar en de groep te veranderen. Ook de umask waarde is van belang; deze bepaalt de standaardpermissies voor nieuw aangemaakte bestanden en directories.
Bij het beheren van gebruikers en groepen heeft elke gebruiker op een Linux-systeem een unieke gebruikers-ID en is lid van ten minste één groep. Het is belangrijk om gebruikers toe te voegen aan de juiste groepen om correcte toegangsrechten te verzekeren. Gebruikers- en groepenbeheer omvat het gebruik van commando's als useradd, usermod, userdel, groupadd, groupmod, en groupdel. Het toekennen van minimale rechten aan gebruikers, volgens het principe van de minste privileges, helpt het risico op ongeautoriseerde toegang te verminderen. De configuratie van sudo is eveneens essentieel. Met sudo kunnen normale gebruikers tijdelijk privileges van de superuser verkrijgen om specifieke commando's uit te voeren. Een veilige sudo configuratie vereist begrip van welke gebruikers, of groepen van gebruikers, welke commando's mogen uitvoeren. Het is ook belangrijk om regelmatig de sudo configuratie en logs te reviseren om te verzekeren dat alleen geautoriseerde gebruikers geprivilegieerde acties kunnen uitvoeren.

Netwerkinstellingen, zoals de firewall

Een fundamenteel aspect hierbij is de configuratie van de firewall, die fungeert als een barrière tussen uw beveiligde interne netwerk en ongeautoriseerde externe netwerken. Een goed geconfigureerde firewall kan de toegang tot het systeem beperken en beschermen tegen ongewenste indringers en netwerkaanvallen. Binnen de Linux-omgeving zijn iptables en ufw (Uncomplicated Firewall) algemeen gebruikte tools voor het beheren van firewall-regels. Iptables maakt deel uit van de oudere generatie firewall-oplossingen, terwijl ufw is ontworpen om de configuratie van firewall-instellingen te vereenvoudigen. Door de beheerder in staat te stellen om toegangsregels effectief te definiëren en te beheren, helpen deze tools bij het vormgeven van het veiligheidslandschap van het systeem. Het is ook belangrijk om bewust te zijn van en begrip te hebben van netwerkprotocollen en poorten, aangezien deze kennis essentieel is bij het configureren van firewall-regels. Het beperken van de toegang tot alleen noodzakelijke poorten en het blokkeren van alle overbodige poorten kan helpen het aanvalsoppervlak van het systeem te minimaliseren en zo de blootstelling aan potentiële dreigingen te verminderen.

Inspectie van de logs

Het inspecteren van logs is een belangrijke vaardigheid om de integriteit van een Linux-systeem te behouden. Logs bieden gedetailleerde informatie over de activiteiten en processen die plaatsvinden op een systeem en kunnen waardevolle inzichten geven in de status van het systeem zowel bij eventuele problemen of beveiligingsincidenten die zich voordoen.
De tail-opdracht is een nuttig hulpmiddel voor het bekijken van logs. Met tail kunnen gebruikers de laatste regels van een bestand bekijken, wat handig is om de meest recente activiteiten of fouten in logbestanden te volgen. Bijvoorbeeld, tail/var/log/syslog zal de laatste tien regels van het syslog-bestand tonen, waarmee recente systeemactiviteiten bekeken kunnen worden. Het cat-commando is ook het bestuderen waard. Het wordt gebruikt om de inhoud van bestanden weer te geven en het is bijzonder handig om snel de gehele inhoud van een logbestand te overzien. Een voorbeeldgebruik zou cat/var/log/auth.log zijn, om authenticatie gerelateerde logs te lezen en te reviewen op tekenen van ongeautoriseerde

toegangspogingen. Voor diepgaande analyse en om specifieke informatie te extraheren, is het grep-commando van onschatbare waarde. Grep kan worden gebruikt om te zoeken naar bepaalde patronen, woorden of zinnen in bestanden, wat praktisch is bij het onderzoeken van specifieke incidenten of activiteiten. Bijvoorbeeld, grep `Failed password' /var/log/auth.log kan worden gebruikt om te zoeken naar mislukte inlogpogingen in het authenticatielog.
Naast het inspecteren van logs, is het ook belangrijk om regelmatig logs te monitoren om ongebruikelijke activiteiten of afwijkingen snel te detecteren. Het instellen van geautomatiseerde logmonitoring en alerting kan ook helpen om snel op de hoogte te zijn van potentiële beveiligingsincidenten.
Op mijn Linux-systemen heb ik altijd een alert die afgaat zodra een gebruiker inlogt via een IP-adres dat niet bekend is; of als admin rechten worden gebruik via het sudo commando.

Herkennen van backdoors

In cybersecurity zijn backdoors toegangspunten in een systeem die door aanvallers worden gebruikt om ongeautoriseerde toegang tot een systeem of netwerk te verkrijgen. Voor Linux-systemen kan het monitoren van de netwerkpoorten die in gebruik zijn, nuttig zijn om potentiële backdoors te identificeren. Zo kun je de commando lsof -i gebruiken om alle applicaties te zien die luisteren naar een poort. Zie je hier in de lijst een poort of applicatie staan die je niet herkent dan zou dat wel eens een backdoor kunnen zijn.
Toch maken veel hackers gewoon gebruik van SSH. Zo zul je soms geen vreemde applicaties zien die luisteren naar poorten waar ze niet naar hoeven te luisteren. cat /var/log/auth.log | grep Accepted | grep -v {IP-adressen die je verwacht}. Op mijn servers heb ik een klein script aanstaan dat me meteen een e-mail stuurt zodra iemand inlogt vanaf een onverwacht IP-adres.
Het beoordelen van systeemprocessen is een essentiële techniek in het identificeren van potentiële backdoors en andere kwaadaardige activiteiten op een Linux-systeem. Dit omvat het analyseren van lopende processen, services en daemons om eventuele ongeautoriseerde of verdachte activiteiten te identificeren. Hier volgt een tweetal commando's van hoe je dit effectief kunt doen:

- ps aux: Dit commando toont een gedetailleerde lijst van de lopende processen. Het kan helpen bij het identificeren van ongebruikelijke of niet-herkenbare processen.
- top/htop: Deze commando's bieden een real-time overzicht van systeemprocessen en hun verbruik van systeembronnen, waardoor snel processen die buitensporige bronnen verbruiken, kunnen worden geïdentificeerd.

Bekijk de commando's en besteed aandacht aan de gebruiker die het proces uitvoert, de CPU en het geheugen dat het verbruikt alsook de commando's die worden uitgevoerd. Verdachte processen kunnen een abnormaal hoog niveau aan systeembronnen verbruiken of onder een onbekende gebruiker draaien. Sommige malware kan processen verbergen. Tools zoals chkrootkit of rkhunter kunnen helpen bij het identificeren van verborgen processen en andere rootkit-functionaliteiten.

Instellen van alerts

Het instellen en de monitoring van je Linux-systeem zorgt ervoor dat je grip houdt op wat er gebeurt. Met de `crontab -e' commando kun je automatisch scripts instellen die ervoor zorgen dat je altijd op de hoogte wordt gehouden als er wat belangrijks gebeurt in jouw Linux-systeem. Heb je meer dan één server staan? Dan kan het goed zijn om te monitoren op backdoors door middel van een centraal logging systeem. Een open source applicatie zoals GrayLog is dan een goede oplossing. Daarnaast kan het gebruik van aanvullende monitoringtools, zoals Nagios of Zabbix, die realtime bijhouden van systeemprestaties en resourcegebruik mogelijk maken, bijdragen aan een meer uitgebreide monitoringstrategie. Deze tools kunnen worden geïntegreerd om je te helpen grip te houden op wat er gebeurt binnen jouw Linux-systeem.

Conclusie

In dit artikel hebben we een grondige duik genomen in de wereld van Linux-beveiliging, waarbij cruciale aspecten zoals systeemhygiëne, veilige configuratie en systeemkennis uitgebreid zijn behandeld. Van het up-to-date houden van systemen tot het nauwgezet beheren van firewall-configuraties en het inspecteren van logs, de versterking van de beveiliging van de Linux-infrastructuur. De besproken tips en tools, indien effectief toegepast, kunnen bijdragen aan het versterken van het robuust maken van een Linux-systeem.

Met dit vijfde artikel sluiten we deze serie af. Wij hebben getracht op heldere wijze de beveiliging voor meerdere operationele systemen te bespreken, zodat de niet specialistische MKB-ondernemer ermee aan de slag kan. Via het PvIB-LinkedInaccount en de e-mailadressen van de auteurs kan u ook toekomstig vragen blijven stellen en problemen voorleggen.