با داکرمی متخصص شوید.

سلام و درود

خب دیگه انتهای فصل لینوکس هستیم حالا لازم داریم که با یه پروژه کوچیک بیشتر با لینوکس کار کنیم و مطالبی که خوندیم رو پیاده‌سازی کنیم. فقط دقت کنید دانش لینوکس خودتون رو همواره بیشتر کنید چون تو ادامه‌ی مسیر همه جا بهش نیاز داریم.

تو این پروژه می‌خواهیم ازتون که یه سرور لینوکس نصب و کانفیگ کنید. لطفا این موارد رو انجام بدید.

- تمام کارها و اقداماتی که انجام می‌دید رو مستند و داکیومنت کنید.
- سیستم‌عامل Debian 12 یا Ubuntu 24.04 رو نصب کنید.
- پارتیشن‌های آن را بر اساس مشخصات زیر ایجاد کنید:

capacity	type	mount	format
2G	Non LVM	/boot	ext4
30G	LVM	/	ext4
30G	LVM	/var	ext4

- ابتدا ابزارهای مورد نیاز خودتون را نصب کنید و پس از آن سرور رو به روز کنید.
- هاردنینگ لینوکس رو انجام بدید به گونه‌ای که بتونید امتیاز بالاتر از ۷۵ در Lynis بگیرید.
- روی سرور سرویس وردپرس به همراه دیتابیس و nginx به عنوان وب سرویس، نصب و کانفیگ کنید. دقت کنید که باید روی خود سرور نصب کنید و از داکر یا سرویس دیگه‌ای برای زیرساخت استفاده نکنید.
- مواردی که لازم است روی nginx کانفیگ شود:
  - سایت مورد نظر حتما از طریق دامنه فراخوانی شود.
  - Gzip روی سایت فعال باشد.
  - ورژن nginx به بیرون expose نشود.
  - بتوانید روی یک sub domain دیگه فایل سرور کنید.
  - برای تمام دامنه‌های خود certificate بگیرید.
  - http به صورت خودکار به https ریدایرکت شود.
  - هدر سکیوریتی HSTS رو ست کنید.
- این موارد رو داخل فایروال لینوکس تنظیم کنید:
  - تنها پورت ssh و پورت ۸۰ و ۴۴۳ به بیرون باز باشد.
  - یک رنج IP رو داخل فایروال وایت‌لیست کنید.
  - رول‌ها رو پرسیست کنید که بعد از ریبوت مجدد آنها لود شود.

با داکرمی متخصص شوید.

- سرور رو طوری کانفیگ کنید که تنها از طریق ssh-key بتوان به آن متصل شد.
- از دیتابیس به صورت برنامه‌ی مشخص و زمان‌بندی شده بکاپ بگیرید. طوری کانفیگ کنید که به صورت برنامه‌ریزی شده این کار تکرار بشود.
- یک دیسک دوم به سرور خود اضافه کنید و ۳۰ درصد آن را به / و مابقی را به var اضافه کنید.
- یک دیسک سوم به سرور خود اضافه کنید و اون رو به عنوان لاجیکال والیوم جدید اضافه و آنرا تو مسیر backup/ مانت کنید و کاری کنید که همواره بعد از ریبوت سرور مانت شود.
- سرویس‌های لینوکس رو تنظیم کنید پس از reboot سرور به صورت خودکار شروع به کار کنند.
- فایل‌های مربوط به وردپرس رو هم در بازه‌های زمانی مشخصی بکاپ کنید.
- بکاپ‌های گرفته شده رو از سرور منتقل و در جای دیگری نگهداری کنید.
- یک یوزر برای تیم مانیتورینگ ایجاد کنید که تنها دسترسی زدن کامند ls و cd را داشته باشد و هیچ کار دیگری نتواند انجام دهد.
- پورت‌های باز سرور را بررسی کنید که پورت اضافی از بیرون در دسترس نباشد.
- سرتیفیکیتی که روی nginx قرار دارد را با استفاده از ssllabs.com بررسی کنید. حتما طوری کانفیگ کنید که رتبه‌ی A به بالا دریافت کند.
- هدرهای سایت را با استفاده از securityheaders.com بررسی کنید. سعی کنید که امتیاز A به بالا را دریافت کنید.
- یک فایل ایجاد کنید که تنها بتوان به آن متن اضافه کرد و نتوان کار دیگه‌ای باهاش انجام داد.
- یک فایل ایجاد کنید که نشه داخل لینوکس با هر دسترسی اون رو پاک یا تغییرش داد.
- یک تسک ایجاد کنید که اولین دقیقه از اولین روز هر هفته یک لیست از دیسک‌ها و حجم استفاده‌شده‌ی آنها تهیه کند و در یک فایلی ذخیره کند.
- یک تسک ایجاد کنید که بعد از هر ریستارت سرور یک سری فایل لاگ رو کپی و به جایی ارسال کند.
- time سرور رو با استفاده از یک ابزاری با تایم سرورهای روی اینترنت سینک کنید. طوری کانفیگ کنید که همواره زمان سرور به روز باشد.
- یک اسکریپت آماده کنید که با استفاده از آن بتوان سرورها و پورت‌های باز آنها را اسکن کرد و در نهایت یک گزارش کامل از آن ایجاد کنید که بتوان آن گزارش رو هر زمان که لازم شد بررسی کرد. لازم است تا این اسکن به صورت برنامه‌ریزی شده در تایم‌های مشخصی از روز انجام شود و حتما گزارش آماده شده در قالب یک سایت با احراض هویت و certificate معتبر در دسترس باشد. باید بتوان گزارش‌های زمان‌های مختلف را جداگانه بررسی کرد.

- اسکریپتی آماده کنید که با استفاده از Trivy سرورها و سرویس‌های آن را اسکن امنیتی کند و در صورتی که آسیب‌پذیری بحرانی داشت حتما آسیب‌پذیری را به همراه زمان و نام سرور و سرویس با ایمیل به یه آدرس اطلاع رسانی کند. این اسکریپت باید ۴ نوبت در طی روز اجرا شود و این موراد کامل خودکار انجام شود. گزارش به دست آمده نیز باید در یک سایتی با احراض هویت و certificate معتبر در دسترس باشد. باید بتوان گزارش‌های زمان‌های مختلف را جداگانه بررسی کرد.