IT-infrastruktur
Individuell inlämning i samband med gruppprojektet
Patrik Khosravi

Virtualisering (Mål 4):
Vår topologi kan beskrivas enklast som betrodda användare
nätverket - Firewall (& ev nginx) VM - Wordpress & DB VM - backup. Allt inom ett ZeroTier-nätverk som skapades och administrerades av Moonlae.

PC-virtualisering med VirtualBox:
Samtliga körde Debian 13.1 för att det var enklast för samtliga gruppmedlemmar.

Servervirtualisering:
Vårt projekt krävde tre separata servrar:

1. **Firewall VM:** Agerade som nätverksgateway med IP-forwarding, NAT-regler och senare nginx reverser proxy
2. **WordPress VM:** Hostade webbapplikation och MariaDB-databas
3. **Backup VM:** Tog emot automatiska säkerhetskopior via SSH

Varje server konfigurerades som egen VM med dedikerade resurser.

Datavirtualisering:
Vi implementerade datavirtualisering genom ZeroTier som skapade ett virtuellt nätverk (10.144.0.0/16) ovanpå den fysiska nätverksinfrastrukturen. Detta gjorde att våra VMs kunde kommunicera säkert trots att de kördes på olika värddatorer.

Resurshantering (Mål 7):
Här gjorde vi inte ett stort jobb men vi resonerade:

- att Wordpress VM behövde vara allsidig då den VirtualBoxen även hostade MariaDB
- att Firewall VM behövde bearbeta mer än lagra så vi lät den köra med 2 kärnor och något mindre diskutrymme än standard
- att backup-VM behövde mer lagringsutrymme än processorkraft så den fick 1 kärna och något mer diskutrymme
- vilket passade bra då vi hade både VM i min VirtualBox.

Sårbarhetsidentifiering (Mål 7):

- Vi lade merparten av vår tid och kraft till att få helheten att funka så vi utförde inte en proaktiv sårbarhetshantering utöver följande:
- Öppen SSH-port (22) mot hela ZeroTier-nätverket - vi begränsade till specifika IP-adresser för att styra flödet.
- WordPress VM tillgänglig direkt på ZeroTier-IP - lade till UFW-regler för att endast tillåta Firewall VM
- Planen var att konfigurera fail2ban i firewall VM + rate limit på en dedikerad reverse proxy server (nginx) om tiden räckte till.
- I efterhand kan vi ha använt oss av nmap för att skanna nätverket.

Hur jag har bidragit till projektet i punktform:

Firewall VM - Konfiguration och Säkerhet:

- Installerade och konfigurerade Debian-baserad Firewall VM i VirtualBox
- Aktiverade IP-forwarding permanent
- Konfigurerade UFW-brandväggsregler för port 80 (HTTP) och 443 (HTTPS)
- Implementerade NAT-regler:
    - PREROUTING DNAT

    - POSTROUTING SNAT
    - MASQUERADE för att ge ZeroTier-enheter internetåtkomst (men tiden räckte inte till för att testa detta)
- Verifierade paketflöde med `tcpdump` via min terminal
- Dokumenterade alla konfigurationssteg

Backup VM - Uppsättning och Automatisering:

- Installerade MariaDB och SSH-server på Backup VM
- Tillsammans med Maya konfigurerade vi SSH-nyckelbaserad autentisering mellan WordPress VM och Backup VM
- Tillsammans med Maya tog vi fram backup-skript på WordPress VM
- Konfigurerade UFW på Backup VM för att endast tillåta SSH från WordPress VM:s IP
- Tillsammans med Maya testade vi backup-process och verifierade att filer anlände korrekt i `/backups/`

Felsökning och Samarbete:

- Med hjälp av Omid och Aryan felsökte vi mellan VMs med ping, curl, tcpdump, iptables kontinuerligt
- Bjöd på kaffe

Dokumentation:

- Sammanställde fullständig konfigurationsguide för brandvägg-VM:et och backup-VM:et
- Dokumenterade alla kommandon och förklaringar