Relembrar:

* nano /etc/network/interfaces
* ss -nltp
* ip -br -c a

SSH:

* apt install openssh-server ou apt-get install…
  + service ssh status | start | stop
  + no cliente: ssh user@[IP]
  + scp file.txt user@... : /home/user/… (copia arquivos do cliente para o server)
* ssh-keygen -t rsa
  + Chave fica salva em ~/.ssh
  + ssh-copy-id user@...
  + No server a chave ssh fica em .ssh, e podemos ver elas no arquivo “authorized keys”
* chmod -v 600 authorized keys
  + Apenas L e E para chaves autorizadas
* + Segurança no SSH:
  + nano /etc/ssh/sshd-config:
    - PermitRootLogin no -> impede conexões ao Root;
    - PasswordAuthentication no -> Apenas SSH;
    - HostBasedAuthentication no ->
    - Mudar a porta de 22 para 2222 ou outras;
    - X11Fowarding no -> Previne sessões X11
    - MaxAuthTries 3 -> Ajuda a prevenir ataques de Brute Force;
    - ClientAtiveInterval 300 -> Desconecta sessões inativas;
    - ClienteAliveCountMax 0 -> Desconecta sessões inativas;

Vulnerabilidade em GET x POST:

* sudo apt update
* sudo apt install php7.4 libapache-mod-php7.4
  + controlado por systemctl
* Os arquivos de GET e POST ficam ou ficarão em /var/www/html
* GET X POST
  + GET: É menos seguro pois os dados ficam expostos na URL e podem ser modificados na mesma.
  + POST: Mais seguro, mas com BURP e FoxProxy podem ser quebrados, por isso é importante usar protocolos como 2FA e encriptação por ex: Bycrypt;
* apt install default-jdk
* apt install burpsuite
  + Settings > Proxies > Add (Title, Type: HTTP, Hostname: 127.0.0.1, Port: 8080)

Ataque de força Bruta (Professor não deu em aula, mas tá no slide)

* sudo apt install mariadb-server mariadb-client
  + controlado por systemctl
  + acessado pelo comando mysql -u root
    - CREATE DATABASE xpto;
    - USE xpto;
    - CREATE TABLE xptoUsers (  
       id INT AUTO\_INCREMENT PRIMARY KEY,  
       username VARCHAR(50) NOT NULL,  
       password VARCHAR(255) NOT NULL  
      ) ;
    - INSERT INTO xptoUsers (username, password) VALUES (‘a’, ‘b’);
    - SELECT \* FROM xptoUsers
    - GRANT ALL PRIVILEGES ON \* . \* TO ‘root’@’localhost’ INDENTIFIED BY ‘ ‘
    - FLUSH PRIVILEGES
  + resetar o DB.
* apt-get install php-mysql
  + reiniciar o apache.