Agenda

- Firewall - bypass firewall and how to defend

ssh port forwarding

- aka ssh tunneling.
- -L: e.g., ssh -L 8000:10.0.2.58:23 seed@10.0.2.5
- encapsulate other TCP protocols inside an established SSH connection
- pros: increases security of any unsecured protocol exchanging data in clear text
- cons: can be abused by attackers or employees to violate security policy

ssh dynamic port forwarding

- -D: e.g., ssh -D 9000 seed@10.0.2.5
- useful when multiple websites are blocked

reverse ssh tunnel

- for evading ingress filtering
- -R: e.g., ssh -R 9000:10.0.2.59:80 seed@10.0.2.5

Defense

- Disable ssh port forwarding: In /etc/ssh/sshd_config, change AllowTcpForwarding to no
- Watch your traffic: ssh tunnels generate more traffic than usual

Reference

A large portion of the material is adapted/copied from:

- Computer Security - A Hands-on Approach by Wenliang Du