JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Identity Exploits

Security Architecture & Tool Sets

Impersonation Attacks

- Attacks takes on the identity of a legitimate user
- Usually involves credential theft or open redirects (OAuth)

Session Hijacking

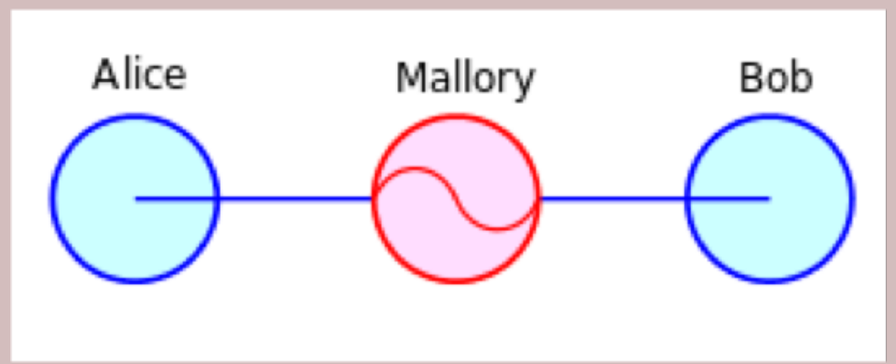
- Attacker takes over an existing session by acquiring or guessing the session key

- Prevented through encrypting sessions

Man-in-the-Middle (MITM)

- Attacker accesses the information flow between systems or services

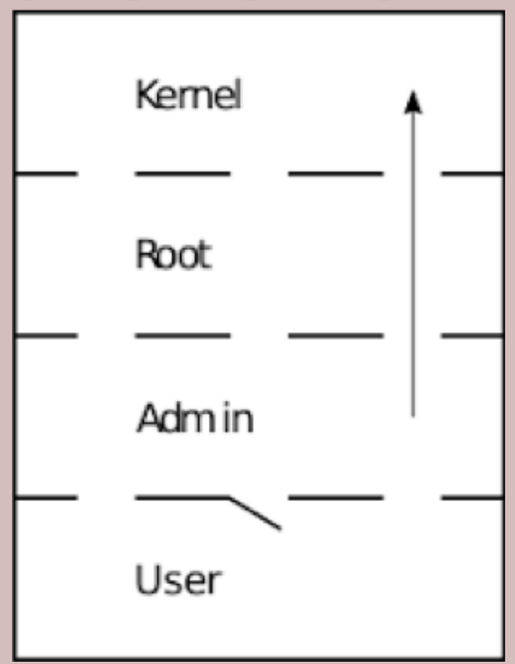
- Prevented through using session or link encryption tunnels



Privilege Escalation

- Attacker elevates their permissions from one level to a higher level

- Usually follows an attack on a normal user account credentials



Rootkits

- Attacker uses malware to provide continued access to a server/client while hiding their own presence

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE