Active Directory Attacks (Bonus)

Ansh Bhawnani

1. Pass-The-Hash

Ansh Bhawnani

Pass-The-Hash

- Instead of cracking passwords, we can dump ***SAM*** database
- Use hashes directly for authentication
- Attacker places the hash into ***LSASS*** section of memory
- Most common target is ***Windows*** (file and printer sharing)

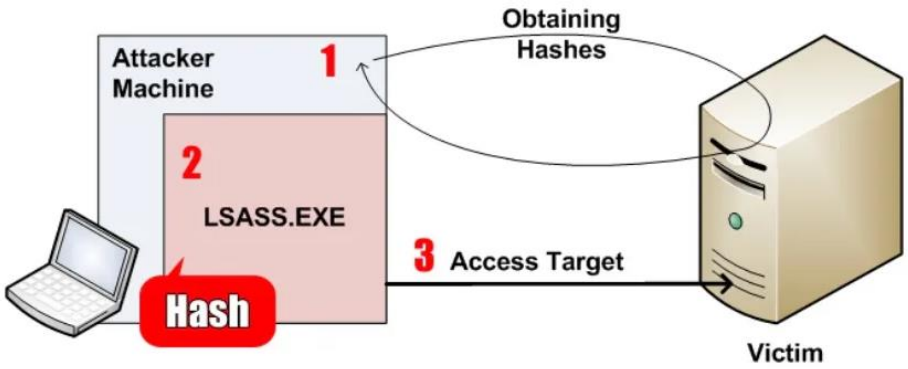
Pass-The-Hash

- **Advantages:**
  - Less time consuming
  - No account lockout
  - Possibly admin privileges

Pass-The-Hash

- **Local Security Authority Subsystem Service (LSASS)**
  - Responsible for enforcing the security policy on the system
  - Verifies authentication creds and keeps the user logged in
  - The system generates and stores a variety of credential materials in *LSASS memory*
  - LSASS contains valuable authentication data such as:
    - *encrypted passwords*
    - *NT hashes*
    - *LM hashes*
    - *Kerberos tickets*

Pass-The-Hash



Pass-The-Hash

- **Mitigations:**
  - *Microsoft Patches 2871997 (Kernels 6.1 – 6.3) for some PTH attacks*
  - *Windows Defender Credential Guard (Only for WIn10 and Server 2016/19)*
  - Fundamental part of network auth and cannot be patched

2. Pass-The-Ticket: Golden Ticket

Ansh Bhawnani

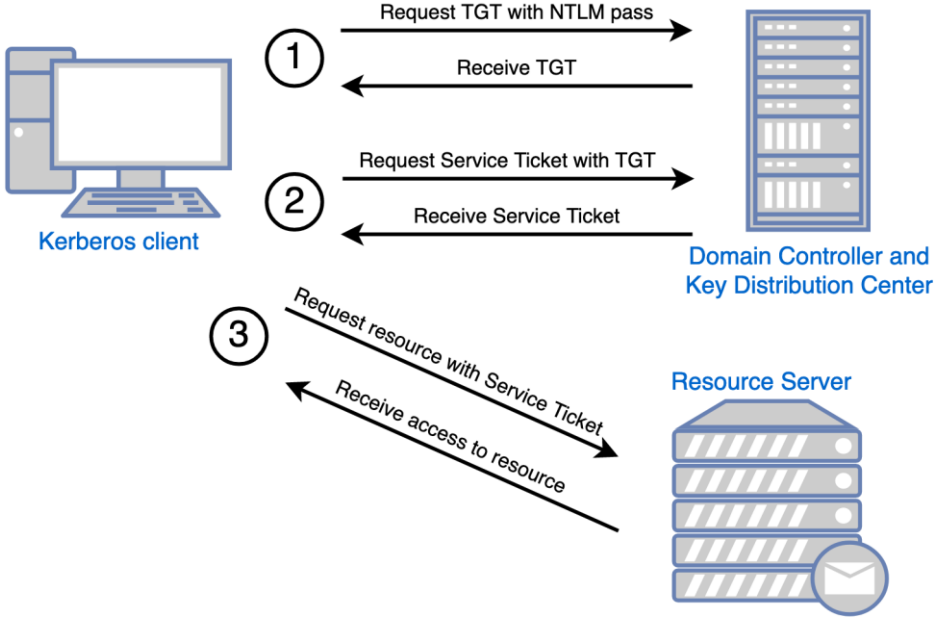
Pass-The-Ticket: Golden Ticket

- **Domain Dominance Technique (AD Persistence)**
- **Ways to Persist Administrative Access:**
  - Dump *ntds.dit*
  - Creation of *domain admin* account
  - Creation of *golden ticket*
  - Creation of *Skeleton key*
  - Use of *DCSync/DCShadow*

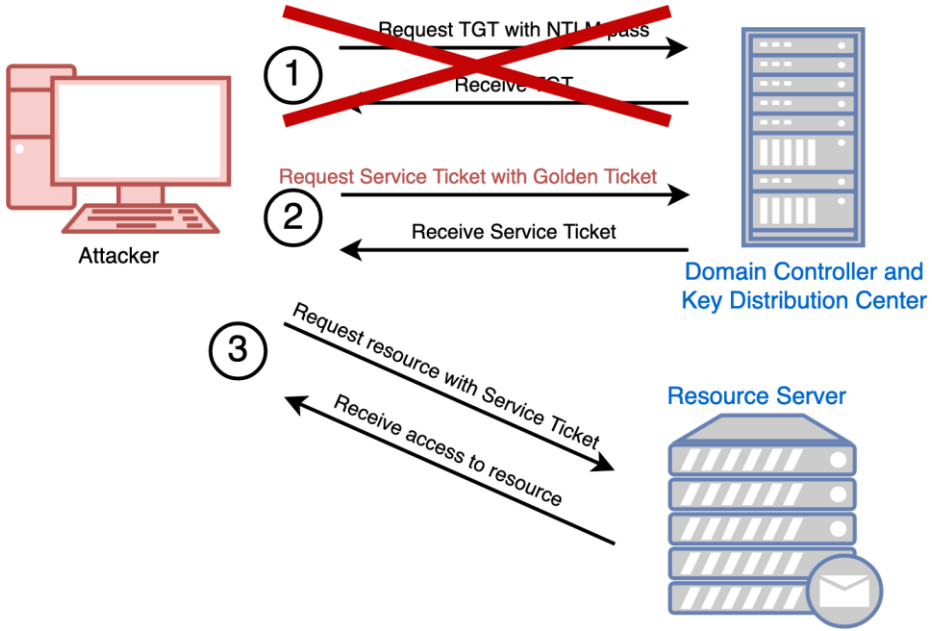
Pass-The-Ticket: Golden Ticket

- It is a special ***Ticket Granting Ticket*** (TGT) providing maximum access for maximum time
- To create a valid TGT (with valid ***PAC***):
  - Target LT Key
  - KDC LT Key
- In case of TGT both are same (***krbtgt NT hash***)
- All other info is mostly public:
  - Domain name,
  - Name of admin account,
  - SID of admin account

Pass-The-Ticket: Golden Ticket



Pass-The-Ticket: Golden Ticket



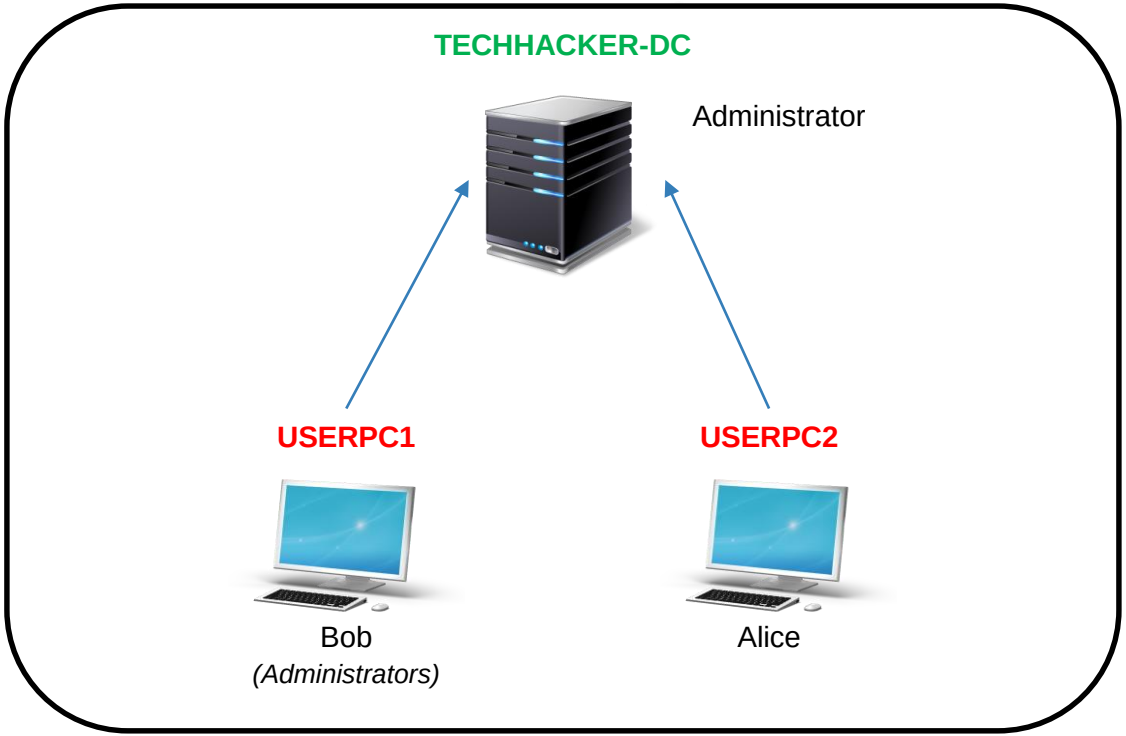
Pass-The-Ticket: Golden Ticket

- **Properties**:
  - Created without interaction with DC (without ***AS-REQ/AS-REP***). Kerberos is a stateless protocol.
  - Requires ***KDC LT Key*** (not easy)
  - It's a TGT for admin account (RID 500)
  - Valid for 10 years by default!

Pass-The-Ticket: Golden Ticket

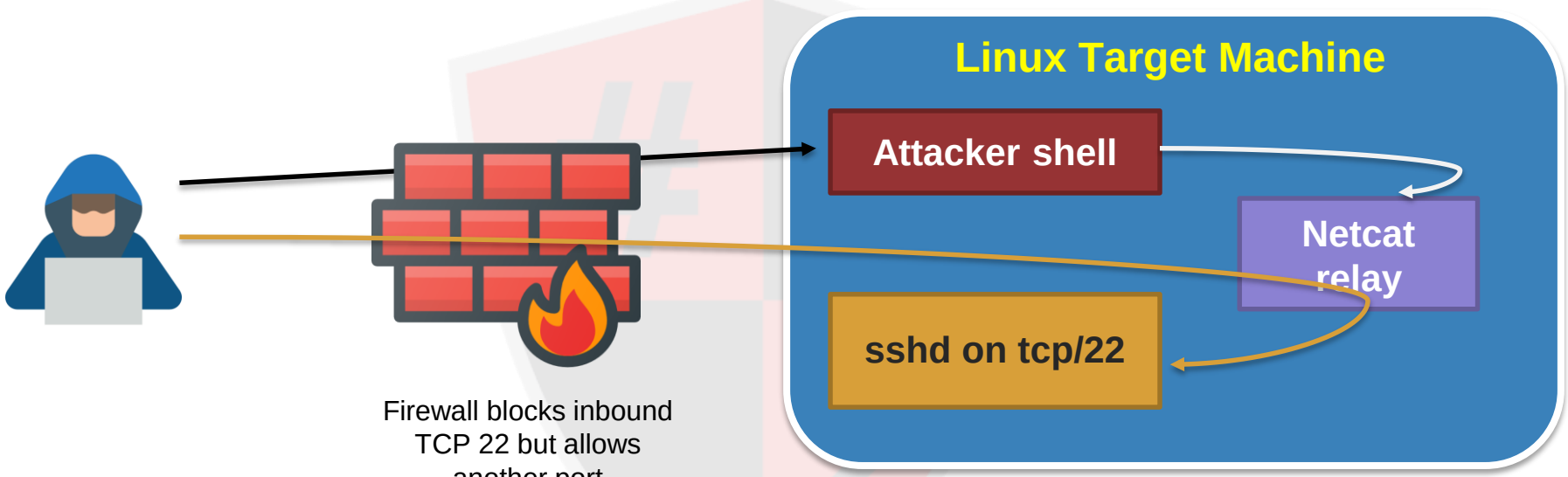
- **Mitigations**:
  - Change the ***krbtgt*** account password TWICE.

Pass-The-Hash



bittentech.local

Port Pivot Relay



Firewall blocks inbound TCP 22 but allows another port

Port Pivot Relay

```
nc -l -p 50000 < mypipe | nc 127.0.0.1 22 > mypipe
```

1 2 3 4

```
nc -l -p 50000 | nc 127.0.0.1 22
```

1 3

HACKING

Is an art, practised through a creative mind.