



Threats to Identity Systems

Security Architecture & Tool Sets

Threats to Identity Systems

- Threats to the underlying authentication and authorization system
 - Exploit how users login
 - How credentials are handled
 - How users are authorized
- Target account lifecycle
 - Creating credentials
 - Preventing credential removal
 - Elevating privileges of credentials
- Attack the account itself
 - Phishing
 - Compromise systems holding credentials



Personnel-based Threats

- Targets users through phishing or social engineering techniques
- User awareness training helps prevent this
- Insider threat would also fall into this category



Endpoint Threats

- Targets your endpoints through...

- Local exploits
- Keyloggers
- Local administrative credentials
- Password stores and tokens



- Protect by using anti-malware and anti-virus
- Protect by using strong authentication stores



Other Identity Threats

- Server-based Threats
 - Attacks your servers to send identity and authentication information to AAA servers
- Application/Service Threats
 - Attacks your applications and/or services that rely on identity and authentication
- Roles, Rights, and Permission Threats
 - Threats focused on users or groups roles, rights, and permissions

