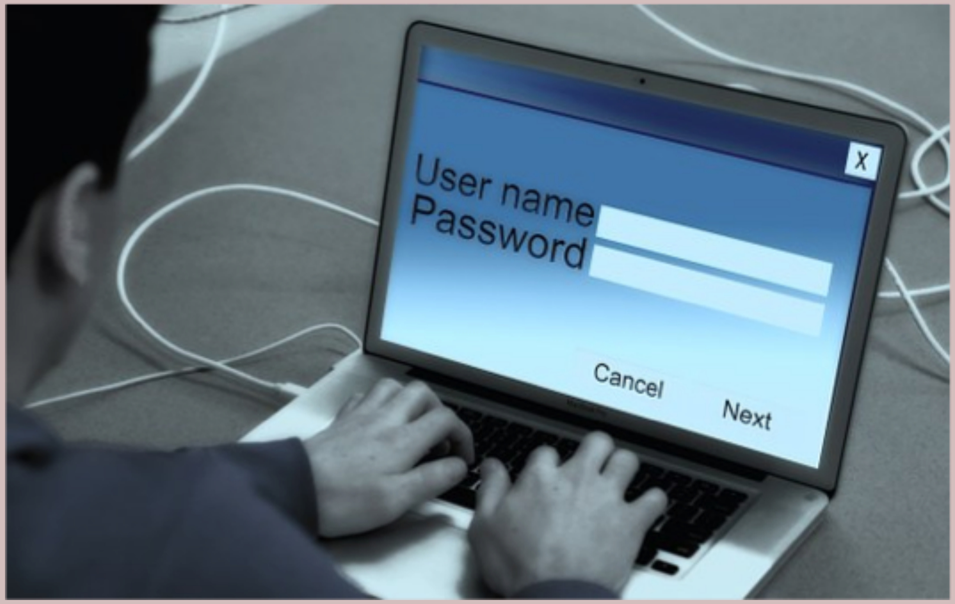
Layered Host Security

Security Architecture & Tool Sets

Layered Host Security

- Servers, desktops, laptops, smartphones are all considered hosts on your network
- Often the most at-risk part of the network since your users directly use them



Common Security Controls

- Passwords and strong authentication
- Encryption (file or full disk)
- Host firewalls and Host-based IPS
- Data Loss Prevention (DLP) software
- Whitelisting/Blacklisting of software
- Antimalware/Antivirus software
- Patch management
- System hardening
- Configuration management
- File Integrity Monitoring
- Logging of events and issues

Cryptography:
Encryption and Hashing

- Encrypting files or the full disk can protect “data at rest”
- Proper storage of the encryption keys/passphrases is critical to security
- Hashing of files can be used to ensure file integrity, as well

Logging, Monitoring, and Validation

- Logs must be securely stored and centrally monitored

- Specialized log server or SIEM (Security Information and Event Management)
  - Tripwire, AlienVault, Splunk, …

- Configuration Management (Microsoft SCCM and others) allow validation of system settings and software across the connected hosts