First 15 min

Firewall setup

In server manager
Right click on “Windows Firewall with Advanced Security” (WFAS) >
Under Domain Profile

- set inbound connections to Block (default)
- Set outbound connections the Allow (default)

For Domain Profile turn on logging

- Log file will be located in C:\Windows\system32\LogFiles\Firewall\pfirewall.log

Open inbound rules

- Disable connections not relate to services running on the machine

AD password changes

For general Windoze machines

Local user account password change (Not for Domain Controller)

Start > administrative tools > computer management > Local users and Groups

- Disable unused accounts
- change all passwords

Make sure you are connected to the domain

(2003) Start > right-click computer > Properties > computer name tab
(2012)

Useful powershell console commands

netstat -ab
kill

Post - 15 min

Downloads

Sysinternals - https://goo.gl/AXD2t1
Password Control for AD - https://goo.gl/6OtKLU
MBSA (Microsoft Baseline security analyzer)
SCW (security configuration wizard)
(SCM) Microsoft security compliance management toolkit
(MSE) Microsoft Security Essentials
Process Hacker
TCPView
Process Explorer
Putty
Wireshark
Autoruns
OSSEC
PeerBlock

Generic

Walk through on setting up AD and DNS:
https://msdn.microsoft.com/en-us/library/ms935682(v=cs.70).aspx
https://msdn.microsoft.com/en-us/library/bb742437.aspx

Win2008

Test box admin password - Neon toaster cat!1
Btables / I'm a password!

AD setup

Server Manager > Roles >

IPSec setup

Group Policy Management

Administrative Tools > Group Policy Management
Right click Domain name > click edit

DNS setup

Click start > open command prompt
Type ipconfig and record IPv4 address

Click start > right click Network > click Properties

In Network and sharing center > click Manage network