Windows Security

Server, Active Directory

(and some general stuff on passwords)

Windows vs Linux

- Windows is commercial, Linux is open source

- Windows software tends to be licensed
- Linux software tends to be open source

- Both can act as a server/workstation
- Both can act as personal computers

- Windows offers paid-support plans
- Linux offers community-driven help

Security 360

Choosing Windows

- The most popular OS
- Windows-dependent software
  - Office365
  - Proprietary software built on Windows
- Hosting a Microsoft Exchange/Skype for Business
- Remote connections
- User friendly workstations for staff
- IT management made easy
  - Disk encryption, access control, policies

Choosing Linux

- Start-ups & small business
  - Low-cost
  - “techy” so happy with the complexity of Linux
- Anyone building software for *NIX

STARTUP WEEK VANCOUVER

Security 360

Windows Critics

- Bloat
  - Lots of background processes
- Black box
  - No one knows what's going on inside
- Security
  - Popularity attracts more exploits
  - Results in lots of ad/malware

Security 360

Windows
Through the Ages

1993 — 2019

- *Personal* & *Personal/Workstation*
  3.1, 95, 98, Me ← **MS-DOS / NT** → XP, Vista, 7, 8, 10
- *Server/Workstation* & *Server-only*
  3.1, 4.0, 2000 ← **NT / NT** → 2003, 2008, 2012, 2016, 2019

Security 360

Powershell

- Windows' answer to the Linux (bash) command-line
- Gives Windows sysadmins programming and automation for servers and server configuration
- Text-based terminal

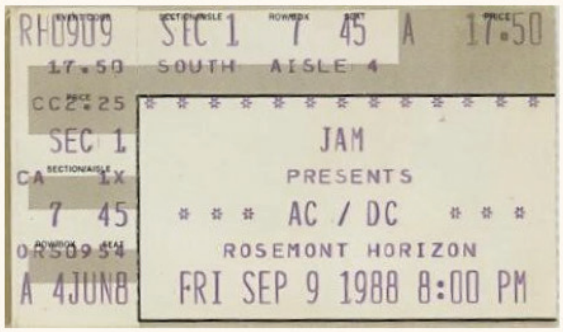
Windows Defender

- Windows Defender Firewall with Advanced Security (WFAS)
  - Host firewall
  - Stateful
  - Deep packet inspection
  - IPSec (think of VPNs)

- Windows Defender Antivirus with Advanced Threat Detection (ATP)
  - Virus, malware, spyware
  - ATP is enterprise/commercial

IT Management

- Active Directory
  - Stores network objects
    - Users
    - Devices
  - Configures these objects
- Domain Controller
  - The server hosting the AD



Security 360

AD Basic Units

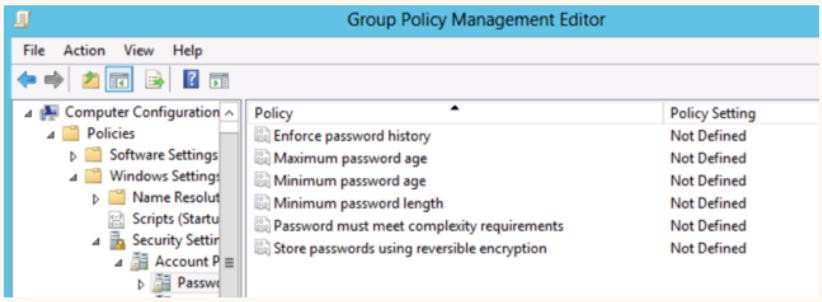
- Users, computers, devices
  - The basic objects in AD
- Groups
  - Collection of basic objects
  - Group in group is also possible
- Organisational Units (OUs)
  - Collection of groups, users, etc...
  - Logical grouping
    - By department / business function

AD in Nature

- Domains
  - Collection of user, groups, OUs
  - All objects that belongs to one DC
  - Gets a *domain name*
- Trees
  - Collection of domains
- Forest
  - Collection of trees
  - Many forests possible

Enforcing Rules

- Group Policy Objects (GPOs)
  - Defines the security configuration for an OU
  - Many, many different settings



A few common GPOs

- Minimum password/passphrase complexity
  - No previously used passwords
  - Lockout restriction
- Modify WFAS rules
- Deny Control Panel access
- Deny Powershell/command-Line access
- Deny USB/Removable Media
- Deny guests
- Deny software installation

Brute-force Attacks

- Offline
  - Try all the possible combinations
  - Write a script to pass them in
  - Feed it with a dictionary file
    - Downloaded or created (CRUNCH)
- Online
  - Different tools for cracking different protocols
  - Username/password must be sent over the wire
    - SSH: Hydra
    - HTTP: Medusa

Hash Attacks

- Password “cracking”

1. Get the hash (can be very difficult)
2. Identify the hash (can also be difficult)
3. Crack the hash (can also be very difficult)
   - Create hashes from a dictionary word-list
   - See if they match your hash

- Better, use Rainbow Tables
  - Pre-computed table matching word-to-hash

Pass-the-Hash Attacks

- Reusing a hash in its encrypted form
  - Get the hash
  - Feed it into the protocol
- Works on Lan Manager (LM) & NTLM hashes
  - Microsoft hashes
  - In < Windows 10 these were easy to extract
  - Windows 10 provides some good hardening, making hashes a lot harder to get

Defences against brute-force

- Policies
  - Set wait times
  - Set maximum password attempt rules
  - Ban obvious attacks

- Ask for something more
  - Use public/private key authentication (SSH)
  - Use 2FA (two-factor authentication)
  - Don’t use passwords! (fingerprint, face)

Not all passwords are passwords

- Something you know
  - This is often the password/passphrase
- Something you have
  - Authenticator/smart card/FOB
- Something you are
  - Face/retinal/fingerprint scans

Defences against hash attacks

- Don't lose your hash
  - Secure it on the server
- Salt your hash
  - Add a bit of data to it which makes rainbow table / PTH attacks inert
- Use a strong hash
  - No MD5 / SHA1
  - Lots of SHA2