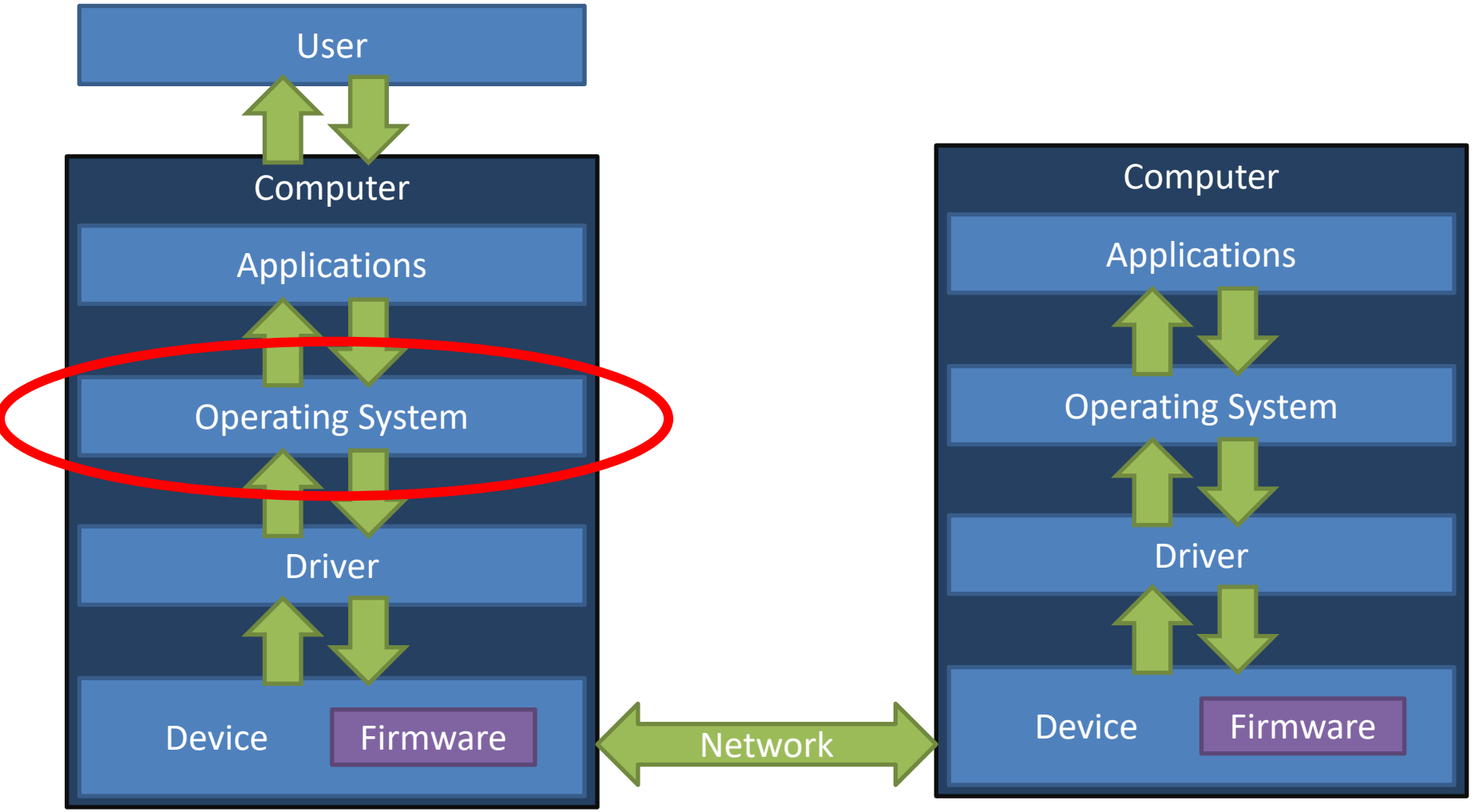
www.crysys.hu

Security Mechanisms in Operating Systems

Gergő Ládi
Laboratory of Cryptography and System Security
Department of Networked Systems and Services
Gergo.Ladi@CrySyS.hu

Introduction



Introduction

- Some relevant topics are not discussed as they have already been discussed on previous subjects or will be discussed later during the semester
  - Memory management, separation of processes (BSc, Operating systems)
  - Basics of AAA and Access Control on Linux and Windows (BSc, IT Security)
  - Specifics of Android and iOS (two separate lectures this semester)
  - Virtualization, containerization (a separate lecture this semester)

- Outline
  - Security in Linux systems
  - Security in Windows systems

SECURITY IN LINUX SYSTEMS

Data Protection

- While the OS implements access control and enforces the policy, it cannot protect against external access
  - An attacker may steal a disk or boot a different OS and read or modify data

- Common solutions
  - Full disk encryption – the entire disk (or partition) is encrypted as a whole
    - » Generally, the boot disk (OS disk) may be protected as well
  - File level encryption – individual files are encrypted

Full Disk Encryption

- Linux Unified Key Setup (LUKS)
  - Encrypts the device in blocks, using a master key
  - The master key is protected by one or more individual keys (separately)
    - Derived from a password (using a KDF)
    - Stored on a media (e.g. pendrive)
    - Stored in the TPM
  - User-configurable algorithms for encryption and integrity protection
  - Transparent operation

- VeraCrypt (TrueCrypt)
  - Open source, cross platform solution
  - Typically used to create virtual, encrypted drives, but may also be used to protect the boot/OS drive

File Level Encryption

- eCryptfs
  - Each file is encrypted using a different FEK (File Encryption Key)
    - » FEKs are protected using one common FEKEK (FEK Encryption Key)
  - Encryption is based on the OpenPGP file format
    - » The metadata is stored in the file itself -> portability
  - File and directory names are also encrypted
  - Used by ChromeOS and Ubuntu's Encrypted Home Directory feature

- EncFS
  - Relies on FUSE -> does not require root
  - Easier to configure
  - Development status: unclear as of Sept 2023

Pluggable Authentication Modules (PAM)

- An authentication framework, available on modern Linux systems
- Applications may rely on PAM instead of having their own authentication logic
- Administrators may define how they would like users to be authenticated
  - Configuration in /etc/pam.conf, /etc/pam.d/*
  - Rules may be set on a program-by-program basis
  - One or more authentication methods may be required
    - » Passwords, keys, LDAP/Kerberos, SAML, …
- Extensibility: custom modules may be written and installed

Pluggable Authentication Modules (PAM)

- Module types
  - Authentication – provides authentication features
  - Account – provides account-related checks
    - » E.g. expired passwords, logon hours
  - Session – provides session-related features
    - » E.g. logging, clean-up on disconnect
  - Password – allows users to change credentials (passwords, keys, …)

- Several modules of the same type may be active at the same time
  - The order of evaluation is sequential but the behaviour may be different based on the control flags

PAM Control Flags

- Required
  - The module must return success for authentication to succeed
  - Evaluation **continues** upon failure
- Requisite
  - The module must return success for authentication to succeed
  - Evaluation **is terminated** upon failure
- Sufficient
  - Authentication failure is ignored
  - Upon success
    - » If no required modules reported failure, terminate with success
    - » If at least one required module reported failure, continue evaluation
- Optional
  - Results only matter if there are only optional modules listed for a given type

Sample PAM Configuration File

```
gergo.ladi@ubuntu2204:~$ cat /etc/pam.d/common-auth
#
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
auth    [success=2 default=ignore]      pam_unix.so nullok
auth    [success=1 default=ignore]      pam_sss.so use_first_pass
# here's the fallback if no module succeeds
auth    requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
auth    optional                        pam_cap.so
# end of pam-auth-update config
```

Capabilities

- System-wide permissions that may be assigned to processes
  - This may help avoid the need to use the root account too frequently
- Examples:
  - CAP_CHOWN – can change ownership information on files/folders
  - CAP_DAC_READ_SEARCH – pass all file system ACL checks for reads
  - CAP_DAC_OVERRIDE – pass all file system ACL checks
  - CAP_KILL – send any signal to any process (not just SIGKILL)
  - CAP_NET_RAW – low-level networking access (e.g. RAW sockets)
  - CAP_SETUID – can arbitarily change UIDs on processes
  - CAP_SETGID – like above, but with GIDs
  - CAP_SYS_ADMIN – mount file systems, set quotas, resource limits, …
  - Use `man 7 capabilities` to read the whole list

```
gergo.ladi@ubuntu2204:~$ sudo getcap /bin/ping
/bin/ping = cap_net_raw+ep
```

Secure Computing Mode (SecComp)

- Processes may enter Secure Computing Mode on request
  `prctl(PR_SET_SECCOMP, SECCOMP_MODE_STRICT);`
- In this mode, only four types of syscalls are allowed
  - exit()
  - sigreturn()
  - read() – using already open descriptors only
  - write() – using already open descriptors only
- Any other kinds of syscalls result in SIGKILL

- Extension: SecComp-BPF (Berkeley Packet Filters)
  - Customizable as to which syscalls to allow
  - Process may ask for a SIGSYS when a violation occurs, giving it a chance to recover
    `prctl(PR_SET_SECCOMP, SECCOMP_MODE_FILTER, &bpf_prog);`

Namespaces

- Namespaces make it possible to isolate processes from other processes and resources in other namespaces
  - The foundation of containerization (LXC, Docker, …)
- Common namespaces
  - net – Isolation of network – NICs can be assigned to namespaces, with each namespace having their own routing tables, firewall rules, etc.
  - user – Isolation of users – Namespaces may have different sets of users, including different root users
  - pid – Isolation of processes – Namespaces cannot see processes in others
  - mnt – Isolation of mount points – File systems mounted in a namespace are not visible from others
  - ipc – Isolation of inter-process communication
  - UTS – The same host may choose to have a different hostname in each of the namespaces
  - cgroup – Isolation of control groups (used for resource allocation)

grsecurity

- A set of kernel patches that aim to make Linux systems more secure
- Features
  - PaX (memory protection)
  - RBAC with automated policy learning
  - Process hiding
  - Stricter *chroot* restrictions
  - More auditing, logging capabilities
  - GCC Plugins
- No longer free as of 2017-04-26

fail2ban

- An optional service that monitors log files and triggers actions when specific criteria are met
  - The log files are typically those of network services
  - The criteria are typically failed login attempts
  - The action is typically blocking ("banning") the user using iptables
- Jail – a set of configuration items
  - Which log file to monitor
  - What to look for
  - What action to take
  - How long to ban for
  - …
- Multiple jails may be active at the same time

SECURITY IN WINDOWS SYSTEMS

BitLocker

- Windows' built-in full disk encryption solution
  - Supported since Windows Vista
  - Not available on Home editions
- Operation
  - Encrypts the contents of the partition using AES-CBC (older versions or compatibility mode) or AES-XTS
  - Protects the encryption key using one or more individual keys
    - » Derived from passwords
    - » Stored in a file or on a pendrive
    - » Stored in the TPM
    - » Derived from a recovery key (printed when BitLocker is set up)
- Transparent operation

Encrypting File System (EFS)

- A built-in file level encryption solution
- Requires a file system that supports metadata (e.g. NTFS or ReFS)
- May be enabled at a file or folder level
  - The latter is preferred

Secret Folder

Secret File.txt

- Operation
  - On first use (per user), an RSA key pair is generated
    - » The key pair is then protected using the user's credentials
  - Each file is encrypted using a symmetric FEK (File Encryption Key)
  - FEKs are protected using the user's RSA key pair
- Transparent operation

Local Security Authority Subsystem

- A service that handles most AAA-related tasks (lsass.exe)
  - Verification of credentials
  - Handling password changes
  - Logging
  - Enforcement of the security policy
- This process must be protected
  - A crash will lead to a system reboot
  - Cached credentials may be stolen from its memory -> could be disastrous
- Extensibility via Security Support Providers (SSPs)
  - Rogue SSP may steal passwords and subvert authentication

Privileges

- Similar to capabilities on Linux
  - But privileges are assigned to users or groups, not processes
- Can be configured using the Local Group Policy Editor or via GPOs (in enterprise environments)

- Current privileges may be listed using `whoami /priv`

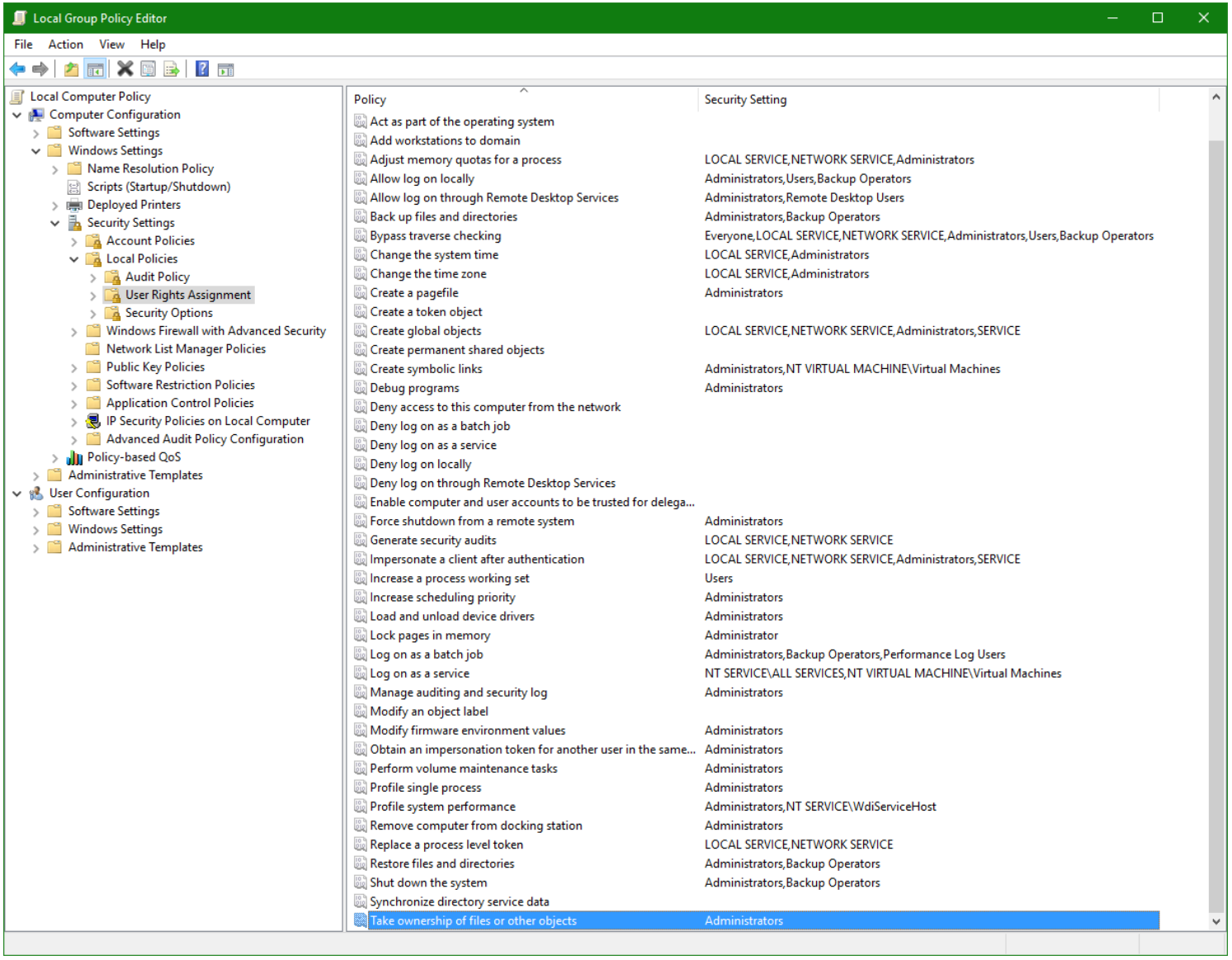
Privileges

```
C:\Users\gergo.ladi\Desktop>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeLockMemoryPrivilege                     Lock pages in memory                                               Disabled
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Disabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Disabled
SeCreatePermanentPrivilege                Create permanent shared objects                                    Disabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Disabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Disabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Disabled
SeTimeZonePrivilege                       Change the time zone                                               Disabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Disabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Disabled
```

Privileges


Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Policy
Security Setting
Act as part of the operating system
Add workstations to domain
Adjust memory quotas for a process LOCAL SERVICE,NETWORK SERVICE,Administrators
Allow log on locally Administrators,Users,Backup Operators
Allow log on through Remote Desktop Services Administrators,Remote Desktop Users
Back up files and directories Administrators,Backup Operators
Bypass traverse checking Everyone,LOCAL SERVICE,NETWORK SERVICE,Administrators,Users,Backup Operators
Change the system time LOCAL SERVICE,Administrators
Change the time zone LOCAL SERVICE,Administrators
Create a pagefile Administrators
Create a token object
Create global objects LOCAL SERVICE,NETWORK SERVICE,Administrators,SERVICE
Create permanent shared objects
Create symbolic links Administrators,NT VIRTUAL MACHINE\Virtual Machines
Debug programs Administrators
Deny access to this computer from the network
Deny log on as a batch job
Deny log on as a service
Deny log on locally
Deny log on through Remote Desktop Services
Enable computer and user accounts to be trusted for delega...
Force shutdown from a remote system Administrators
Generate security audits LOCAL SERVICE,NETWORK SERVICE
Impersonate a client after authentication LOCAL SERVICE,NETWORK SERVICE,Administrators,SERVICE
Increase a process working set Users
Increase scheduling priority Administrators
Load and unload device drivers Administrators
Lock pages in memory Administrator
Log on as a batch job Administrators,Backup Operators,Performance Log Users
Log on as a service NT SERVICE\ALL SERVICES,NT VIRTUAL MACHINE\Virtual Machines
Manage auditing and security log Administrators
Modify an object label
Modify firmware environment values Administrators
Obtain an impersonation token for another user in the same... Administrators
Perform volume maintenance tasks Administrators
Profile single process Administrators
Profile system performance Administrators,NT SERVICE\WdiServiceHost
Remove computer from docking station Administrators
Replace a process level token LOCAL SERVICE,NETWORK SERVICE
Restore files and directories Administrators,Backup Operators
Shut down the system Administrators,Backup Operators
Synchronize directory service data
Take ownership of files or other objects Administrators

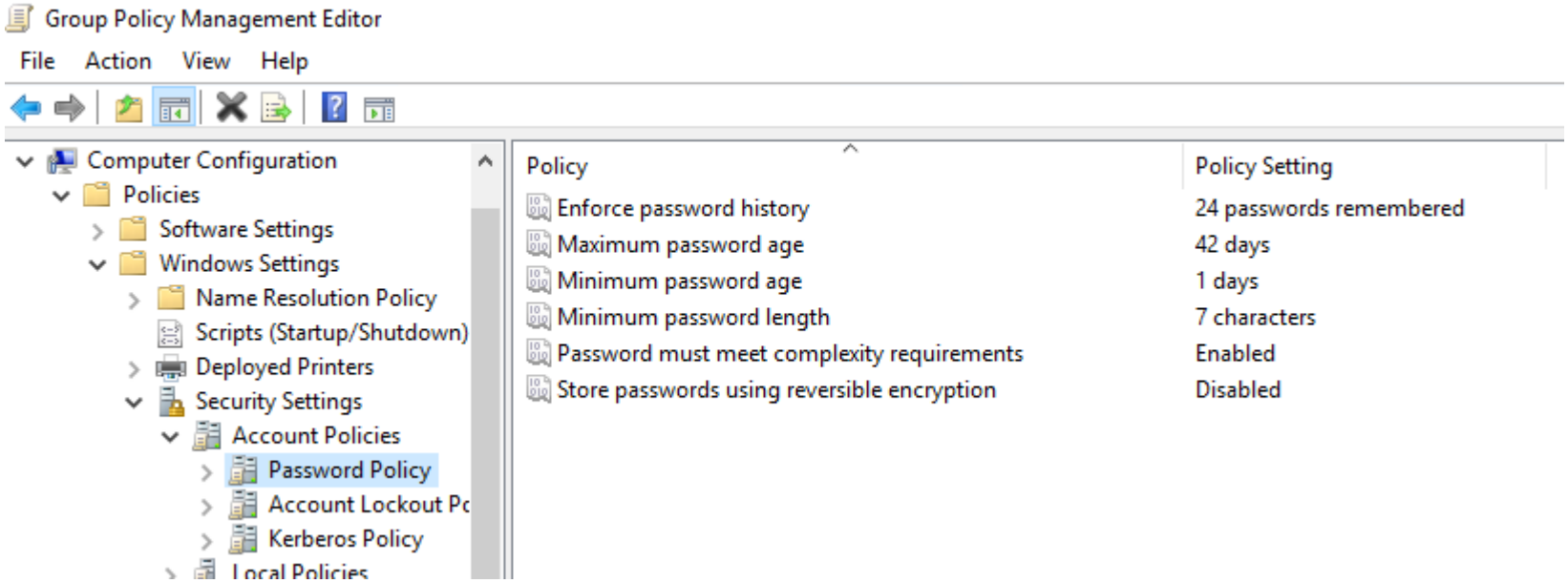
Group Policies

- Used in enterprise environments to distribute settings (including security settings) to large amounts of computers

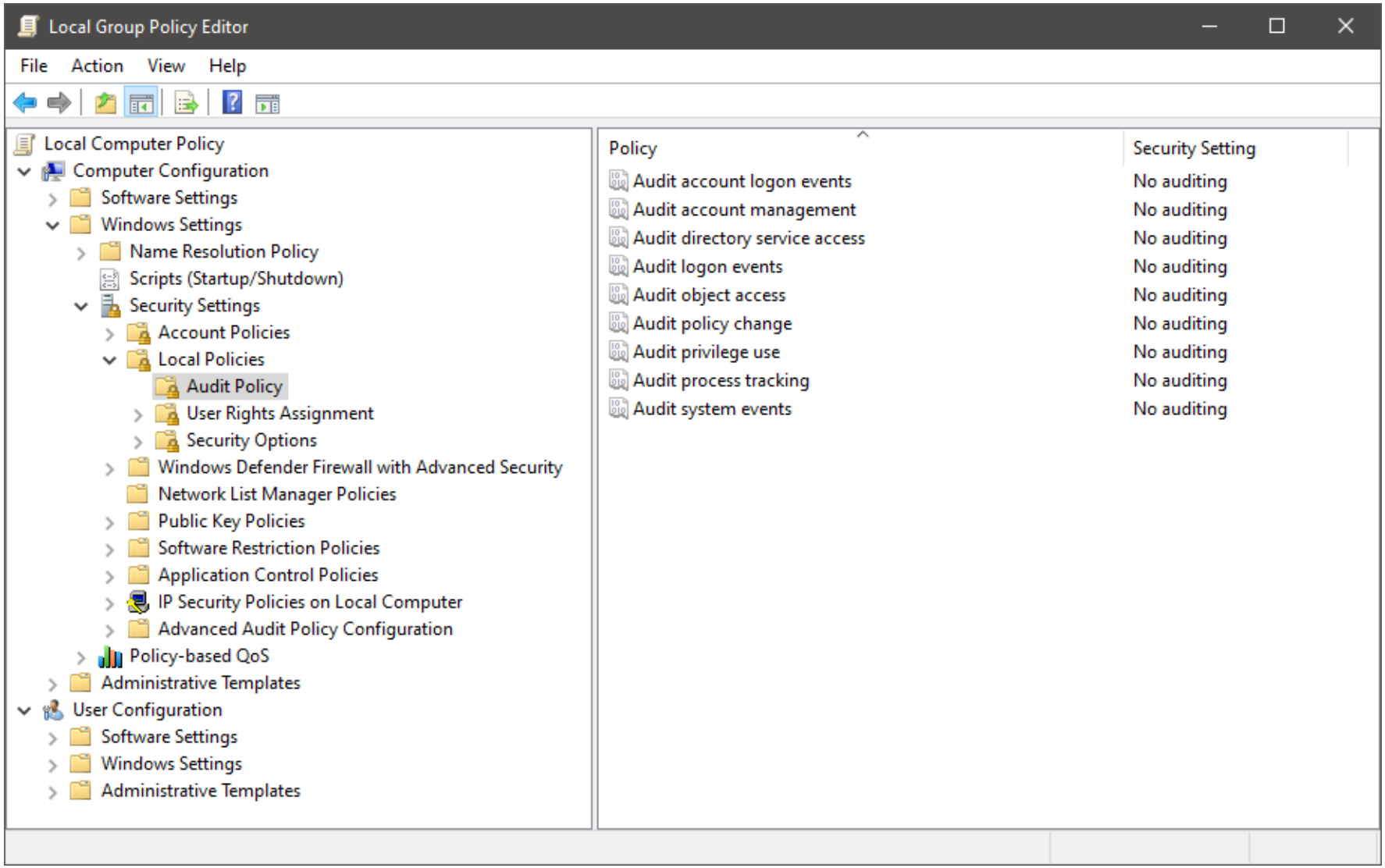
- Group Policy Object (GPO) – a group of settings
- May be linked to specific points in the domain hierarchy

- Configuration items
  - Computer configuration – settings that apply to computers
  - User configuration – settings that apply to users
- Item types
  - Policy – mandatory and is enforced by the system
  - Preference – administrators set an initial value that may be overridden

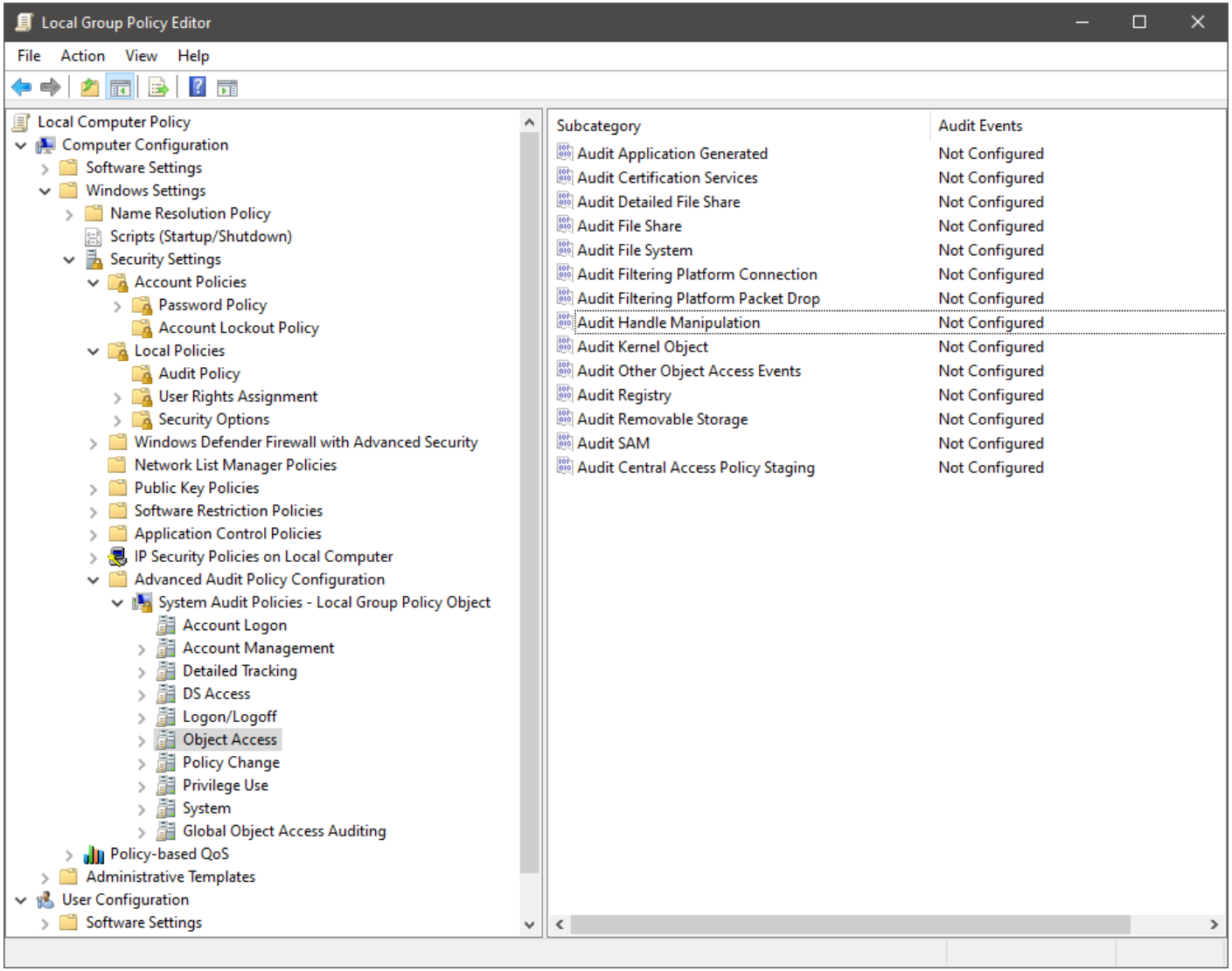
Group Policies – Password Policy



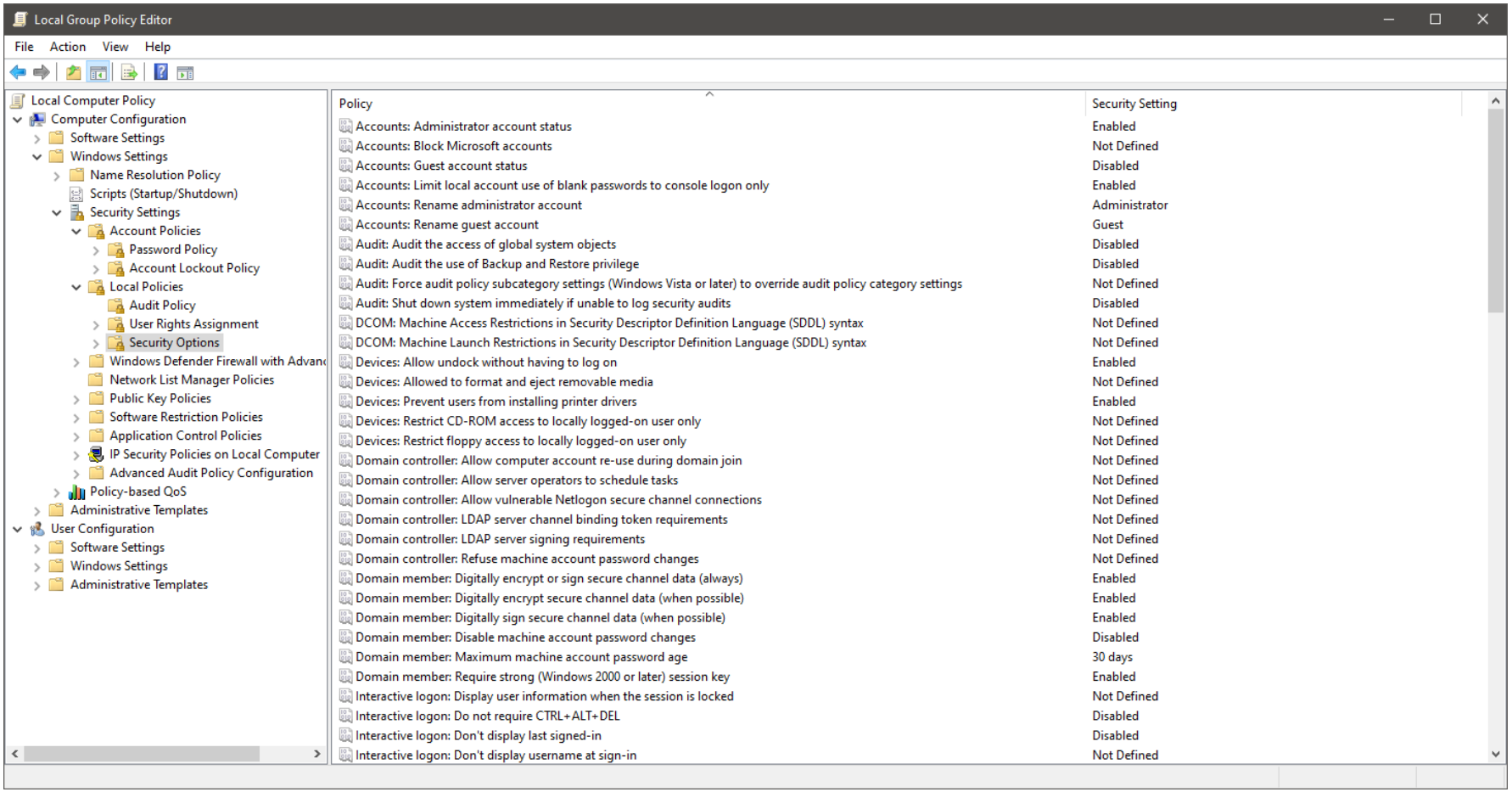
Group Policies – Audit Policy



Group Policies – Audit Policy



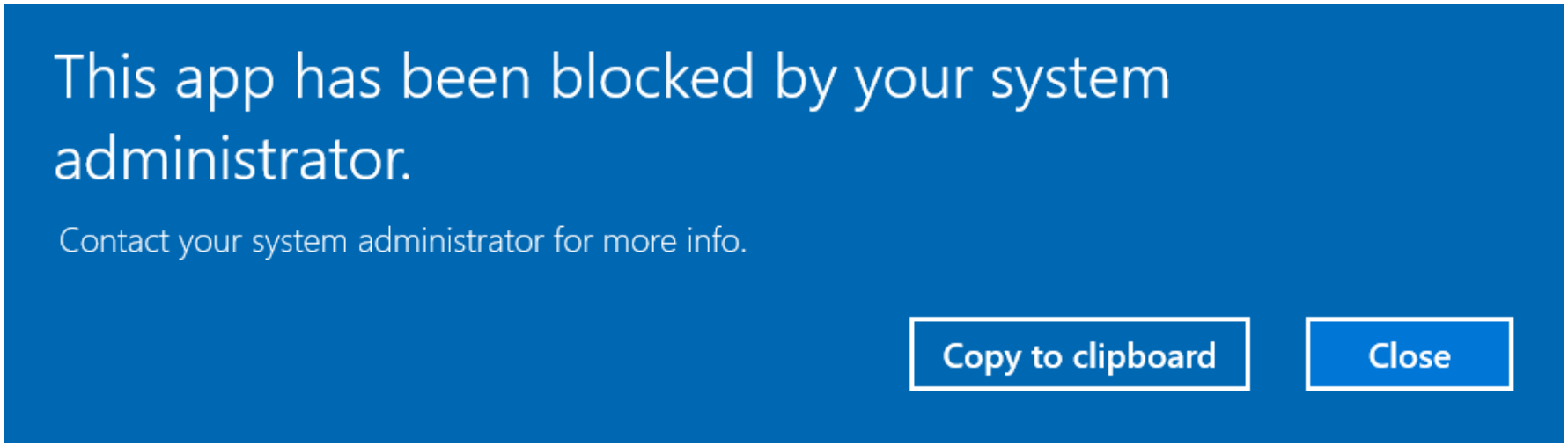
Group Policies – Security Options



AppLocker

- Lets administrators control which applications may be started

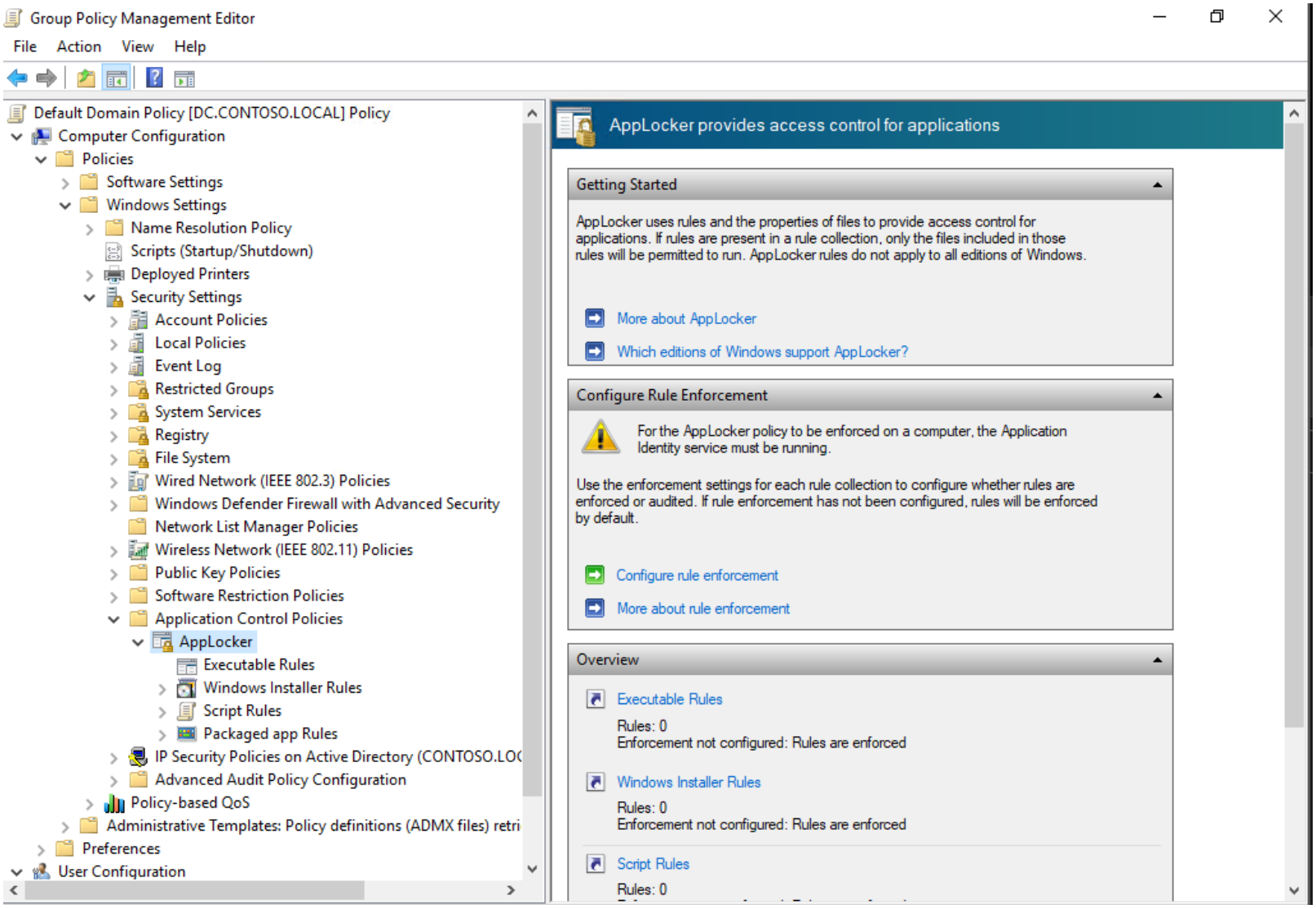
- Approaches
  - Blacklist (relatively easy to bypass)
  - Whitelist (preferred)



AppLocker

- Rules may be defined
  - Manually
  - By running a scan on a known good installation
- Applications may be filtered using
  - Path and name
  - Publisher (name, product name, file name, file version)
  - File hash
- The Application Identity service must be running on the computers

AppLocker


Group Policy Management Editor
File Action View Help
Default Domain Policy [DC.CONTOSO.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
AppLocker
Executable Rules
Windows Installer Rules
Script Rules
Packaged app Rules
IP Security Policies on Active Directory (CONTOSO.LOC
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files) retri
Preferences
User Configuration
AppLocker provides access control for applications
Getting Started
AppLocker uses rules and the properties of files to provide access control for applications. If rules are present in a rule collection, only the files included in those rules will be permitted to run. AppLocker rules do not apply to all editions of Windows.
More about AppLocker
Which editions of Windows support AppLocker?
Configure Rule Enforcement
For the AppLocker policy to be enforced on a computer, the Application Identity service must be running.
Use the enforcement settings for each rule collection to configure whether rules are enforced or audited. If rule enforcement has not been configured, rules will be enforced by default.
Configure rule enforcement
More about rule enforcement
Overview
Executable Rules
Rules: 0
Enforcement not configured: Rules are enforced
Windows Installer Rules
Rules: 0
Enforcement not configured: Rules are enforced
Script Rules
Rules: 0

Windows Defender Exploit Guard

- New feature as of Windows 10 v1709
- Four components
  - Network Protection
    - » URL/IP-based filter that blocks outgoing connections
  - Controlled Folder Access
    - » Blocks unknown applications from accessing Protected Folders
      - The list is customizable, includes Documents and similar folders by default
  - Attack Surface Reduction
    - » Blocks suspicious JavaScript, VBScript and PowerShell scripts
    - » Prevents Office apps from forking, injecting code, and some macro functionality
  - Exploit Guard
    - » Enables various memory and program integrity checks

MISCELLANEOUS

Further Reading

- The Linux-PAM System Administrators' Guide
  http://www.linux-pam.org/Linux-PAM-html/Linux-PAM_SAG.html
- A seccomp overview
  https://lwn.net/Articles/656307/
- capabilities(7) - Linux man page
  https://linux.die.net/man/7/capabilities
- Grsecurity goes private
  https://lwn.net/Articles/721848/
- Péter Gombos: LM, NTLM, Net-NTLMv2, oh my!
  https://medium.com/@petergombos/lm-ntlm-net-ntlmv2-oh-my-a9b235c58ed4
- Privilege Constants
  https://docs.microsoft.com/en-us/windows/desktop/secauthz/privilege-constants
- Attack Surface Reduction feature in Windows Defender
  https://www.thewindowsclub.com/attack-surface-reduction-windows-defender

Control Questions – General & Linux

- Explain the purpose and typical operation of full disk encryption.
- Explain the purpose and typical operation of file level encryption.

- What is LUKS? Explain how it works.
- What file level encryption solutions do you know that work on Linux? How do these work?
- What is PAM? What is its purpose, how does it work?
- Explain what Capabilities are.
- What is SecComp?
- Explain the purpose of Namespaces.
- What is fail2ban? How does it work?

Control Questions – Windows

- What is BitLocker? Explain how it works.
- Explain what the Encrypting File System is and how it works.
- What is the LSASS? Why is it important to protect its process?
- Explain what Privileges are in Windows and why they are important from a security point of view.
- What are Group Policies? How can you use GPOs to improve security in your organization?
- Explain what AppLocker is and how it works.

THANK YOU FOR YOUR ATTENTION!