Mandatory Access Control Essentials with SELinux

Costas Senekkis

INTERNATIONAL CYBERSECURITY INSTITUTE

Agenda

- **Objectives:**
- About Me
- What SELInux is
- SELinux Modes
- Discretionary Access Control
- Mandatory Access Control
- SELinux Policies
- SELinux Labels
- Type Enforcement
- Examples

INTERNATIONAL CYBERSECURITY INSTITUTE

About Me

- Senior Security Consultant at ICSI UK
- Penetration Testing Team Leader
- Deliver training for Penetration Testing around the globe
- Passionate about Linux Security

INTERNATIONAL CYBERSECURITY INSTITUTE

What SELinux is

- An additional layer of system security
- Not an antivirus nor a firewall, IDS/IPS
- A set of patches to the Linux kernel using Linux Security Modules (LSM)
- Adopted from the kernel version 2.6.0 in 2003
- Primary goal is to protect data from services that have been compromised

SELinux Modes

- **Enforcing** – Denies Access so system services that attempt to read files with incorrect type context
- **Permissive** – Used for troubleshooting. Allows all interactions and logs interactions that would be denied in enforcing mode.
- **Disabled** – Disables completely SELinux

Discretionary Access Control

- Unix/Linux systems use discretionary access control
- Permissions of user, group and others. (Ownership)
- Users can change permissions on their own files (chmod)

Mandatory Access Control

- Mandatory Access Control (MAC) is based on security labels.
- Is managed by a central authority not by an individual (owner of the object)
- Example:
  - By changing permissions on a file (DAC), if there is a policy enabled preventing users or processes accessing that file, then you are safe

SELinux Policies

- Targeted – Default Policy
- SELinux Protects targeted processes only
- /usr/bin/sestatus
- /usr/sbin/getenforce
- /etc/selinux/config

SELinux Labels

- Security Labels = SELinux Context
- Context is simply a name used by SELinux and always ends with _t.
- Files, processes, directories and ports have labels
- Labels have the format of user:role:type:level

Type Enforcement

- Part of a policy that permits a system service to access files and directories
- Example:
  - Apache process (httpd_t) can access files and directories under /var/www/html (httpd_sys_content_t)

Examples

- Example with Apache Web Server

Q & A

- Questions????