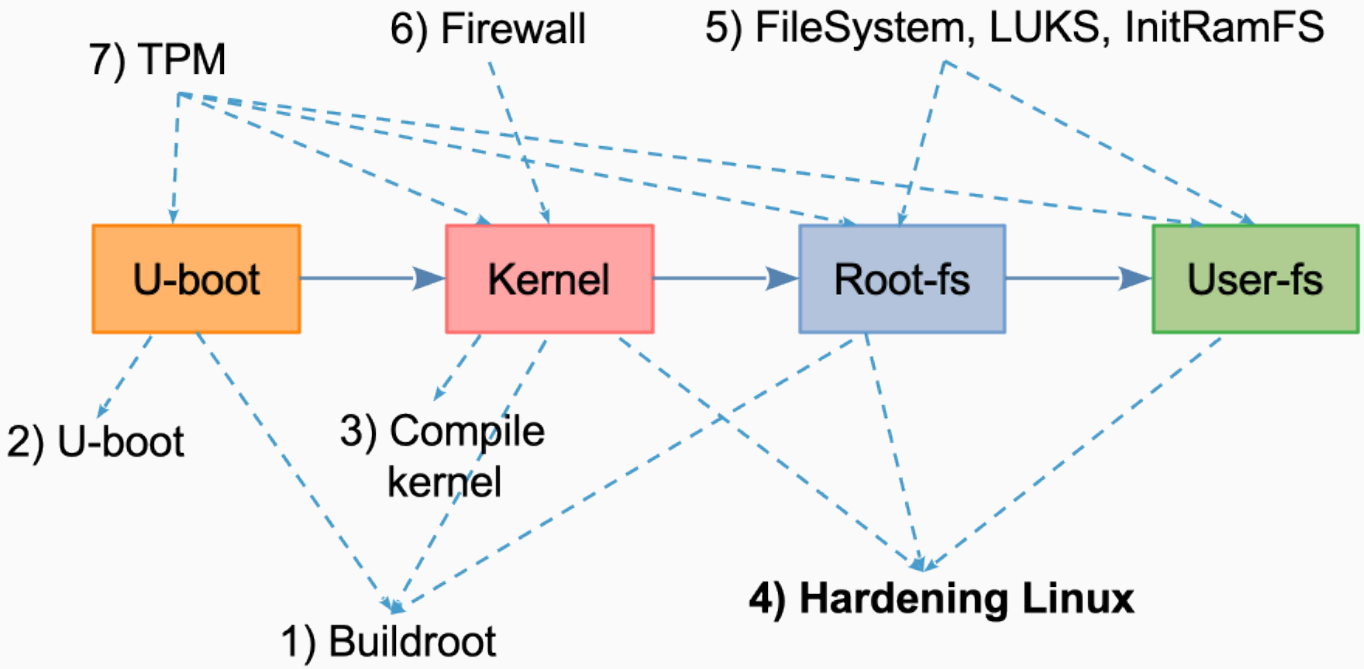
MSE | MASTER OF SCIENCE IN ENGINEERING

MA_SeS - Short track to OSSTMM

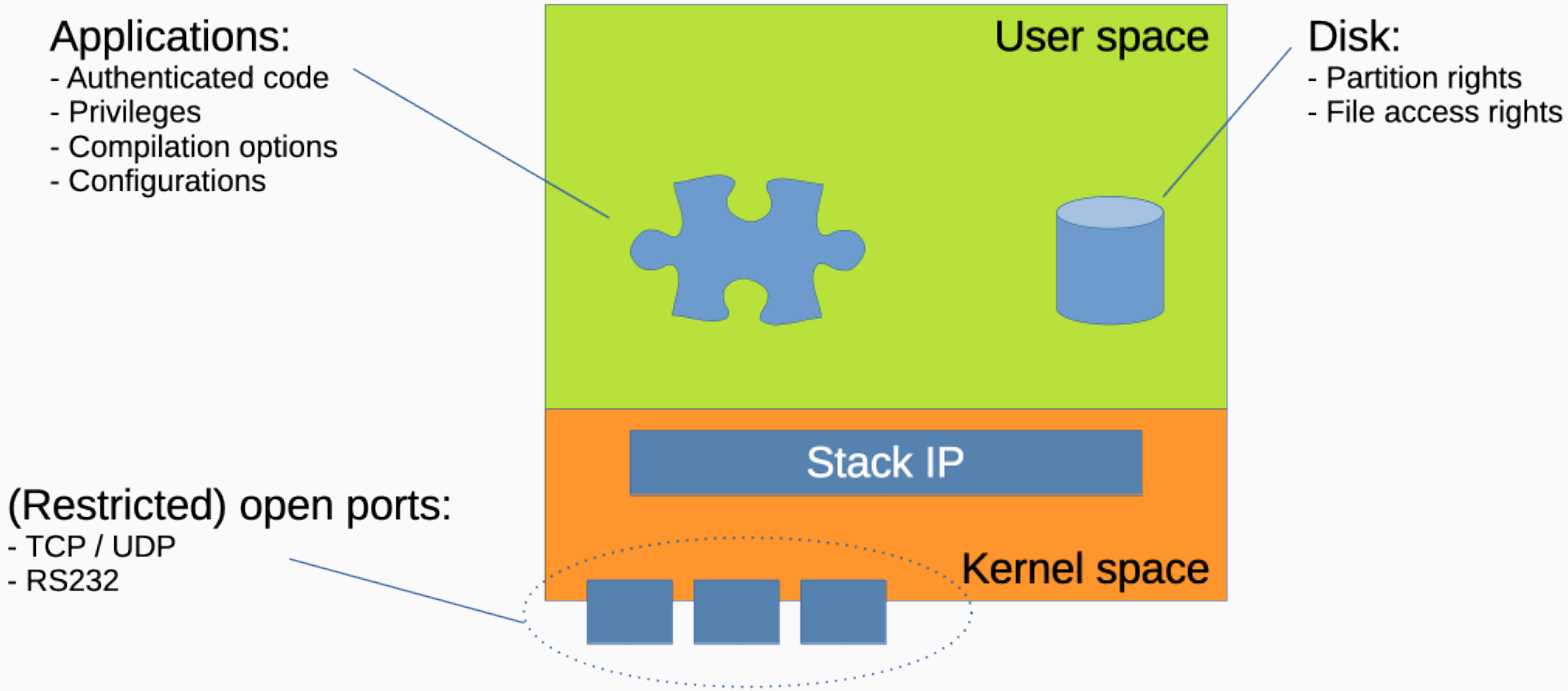
Luca Haab, Michael Mäder, Florent Glück

October 23, 2025

Overview


7) TPM
6) Firewall
5) FileSystem, LUKS, InitRamFS
U-boot
Kernel
Root-fs
User-fs
2) U-boot
3) Compile kernel
4) Hardening Linux
1) Buildroot

Summary


Applications:
- Authenticated code
- Privileges
- Compilation options
- Configurations
User space
Disk:
- Partition rights
- File access rights
Stack IP
(Restricted) open ports:
- TCP / UDP
- RS232
Kernel space

Simplified OSSTMM security testing methodology

IT security check — OSSTMM methodology

Source: https://www.isecom.org/OSSTMM.3.pdf

- The Open Source Security Testing Methodology Manual (OSSTMM) provides a methodology for a thorough security test.
- The OSSTMM encompasses test from all channels – Human, Physical, Wireless, Telecommunications, and Data Networks.
- A set of security metrics, called **Risk Assessment Values (RAVs)**, provides a powerful tool that can provide a graphical representation of state, and shows changes in state over the time.

IT security check — OSSTMM methodology

- This integrates well with a ‘dashboard’ for management and is beneficial for both internal and external testing

OSSTMM — Risk Assessments Values (RAVs)

- The Risk Assessment Value is derived from three categories:
  - Operational Security
  - Loss Controls
  - Security Limitation
- The RAV has 18 different inputs
- The RAV equation requires that each of the categories be assigned a logarithmic base value to scale the three factors of

Category		Input
Operational Security		Visibility
		Access
		Trust
Loss Controls	Class A	Authentication
		Indemnification
		Resistance
		Subjugation
		Continuity
	Class B	Non-Repudiation
		Confidentiality
		Privacy
		Integrity
		Alarm
Security Limitations		Vulnerability
		Weakness
		Concern
		Exposure
		Anomaly

OSSTMM — Risk Assessments Values (RAVs)

Actual Security in accordance with the scope.

- The RAV of Actual Security is a value between 0-100. 100 the maximum security

Simplified OSSTMM (1/2)

OSSTMM method is too detailed for embedded systems. Only the main points of the RAVs are presented:

- **Access**: Count each access which potentially allow interaction with the embedded system. Count each TCP/UDP ports really open

```
nmap -Pn -n -p 1-65535 IP
nmap -Pn -n -sU -p 1-65535 IP
netstat -atunp
```

- **Authentication**: Count each connection to a system (ssh, console, ...) which asks a username and password
- **Confidentiality**: Count each each connection where the data is encrypted. Example: it is better to have only a ssh connnection than a telnet connection to a system

Simplified OSSTMM (2/2)

- **Vulnerability, Weakness, Concern**:
  - Check if a version of a program has vulnerabilities. See these sites: https://www.cvedetails.com/, https://www.cve.org/, https://attackerkb.com/, https://www.exploit-db.com/
  - Check the authentication passwords. The passwords are stored in /etc/shadow, you can use hashcat, John the Ripper, hydra programs in order to check the passwords
  - Check the robustness of the cryptographic algorithms
- **Exposure**: Give direct or indirect unjustified visibility of targets
  - Example: Banner of a services

```
nmap -Pn -n -p 22 -sV IP  // indicate the service version (Openssh 8.1p)
```

Summary of nmap commands


```
From 192.168.0.4:

nmap -sV -PN -n -p 1-65535 192.168.0.11          // scan all tcp ports, with software version
nmap -sU -PN -n -p 1-65535 192.168.0.11          // scan all udp ports, with software version
```

nmap - NSE scripts (1/2)

- nmap has a powerful scripting engine (NSE) which can be used to detect a wide range of information and security vulnerabilities
- Complete documentation of NSE scripts can be found here: https://nmap.org/book/nse-usage.html
- The scripts are stored in `/usr/share/nmap/scripts/` folder
- Example of useful scripts:
  - `ssh-auth-methods.nse`: enumerate supported authentication methods on SSH servers
  - `http-enum.nse`: enumerate directories used by web servers
  - `ftp-anon.nse`: check for anonymous FTP login allowed
  - ... browse the folder for a complete list of scripts

nmap - NSE scripts (2/2)

```
$ nmap --script-help ssh2-enum-algos
ssh2-enum-algos
Categories: safe discovery
http://nmap.org/nsedoc/scripts/ssh2-enum-algos.html

$ nmap --script ssh2-enum-algos 192.168.0.11
PORT   STATE SERVICE
22/tcp open  ssh
| ssh2-enum-algos:
|   kex_algorithms: (6)
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       …
```

end of presentation