Low-hanging fruit

The over-familiar low hanging fruit framed in a simplified structured attack featuring the basics of hacking, as in, “anyone can do it”:

- Footprinting
- Scanning
- Enumeration
- Acquiring access
- Privilege escalation
- Backdoors
- Hiding tracks

Mitigations

- Human error, negligence and ignorance are responsible for a high proportion of data breaches. By all means possible, encourage a culture that is more aware and inspires people to, for example, not click on suspicious web links or attachments, and developers to integrate security tactics into the entire software development lifecycle.
- Many attacks compromise user details and harness genuine user login and password credentials to insert malware and steal data. Strengthen the authentication process.
- For sysadmins, share experiences on discovered threats and methods of neutralising them with peers to assist in both prevention of and dealing with breaches.
- Encrypting all sensitive data at rest and in transit can make it more difficult for hackers to intercept and decipher, especially on mobile devices.
- In an increasingly cloudy world of multiple fixed and wireless cloud-connected PCs, smartphones and tablets, working on protecting servers and routers and employing E2EE encryption does not suffice. Vulnerable endpoints are a major potential risk of data compromise because they can be accessed from the outside without permission or knowledge by those responsible. Additional end-point protection puts security on every device attached to the network.

---

threats, threat-modelling, quick, dirty, example, fruit