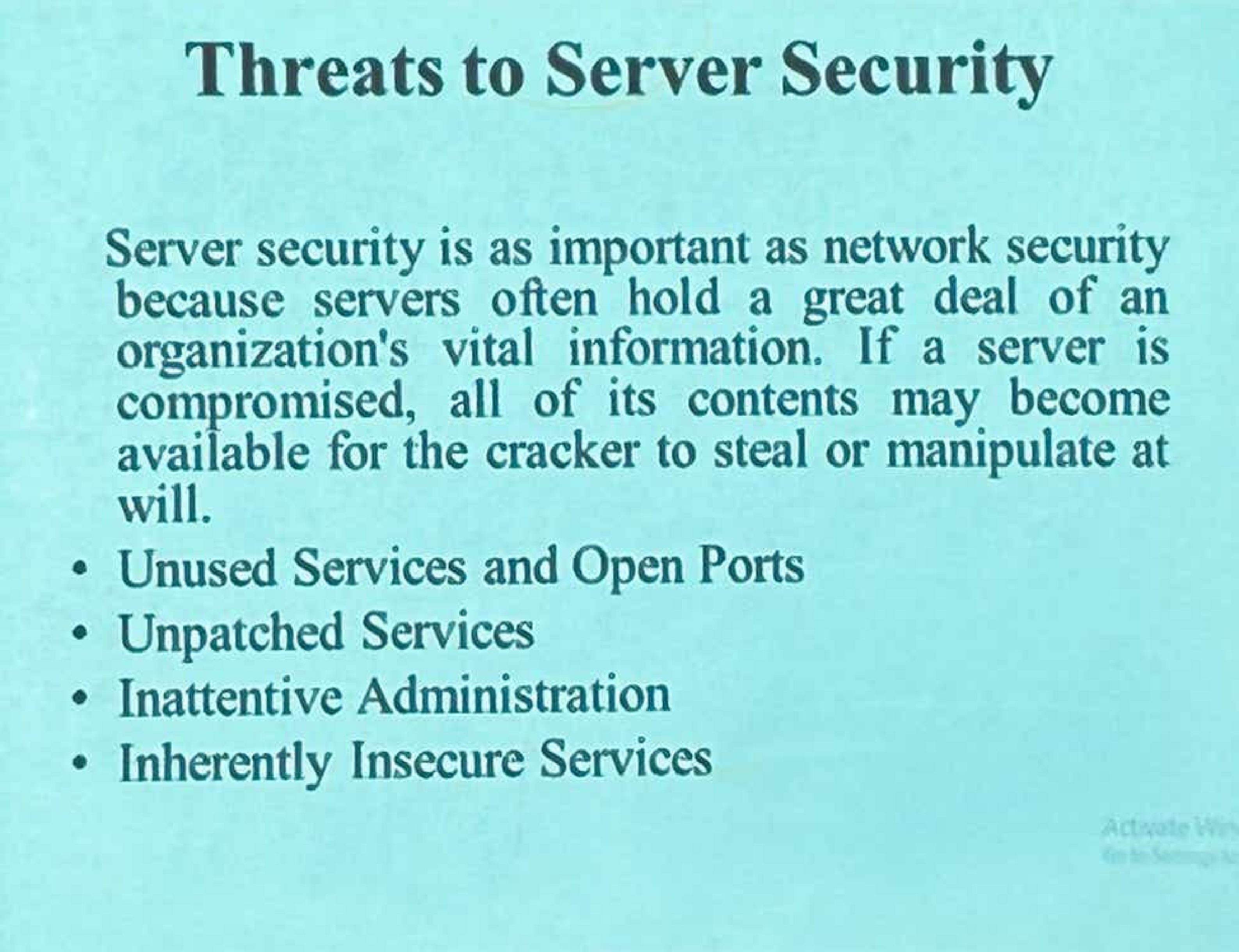
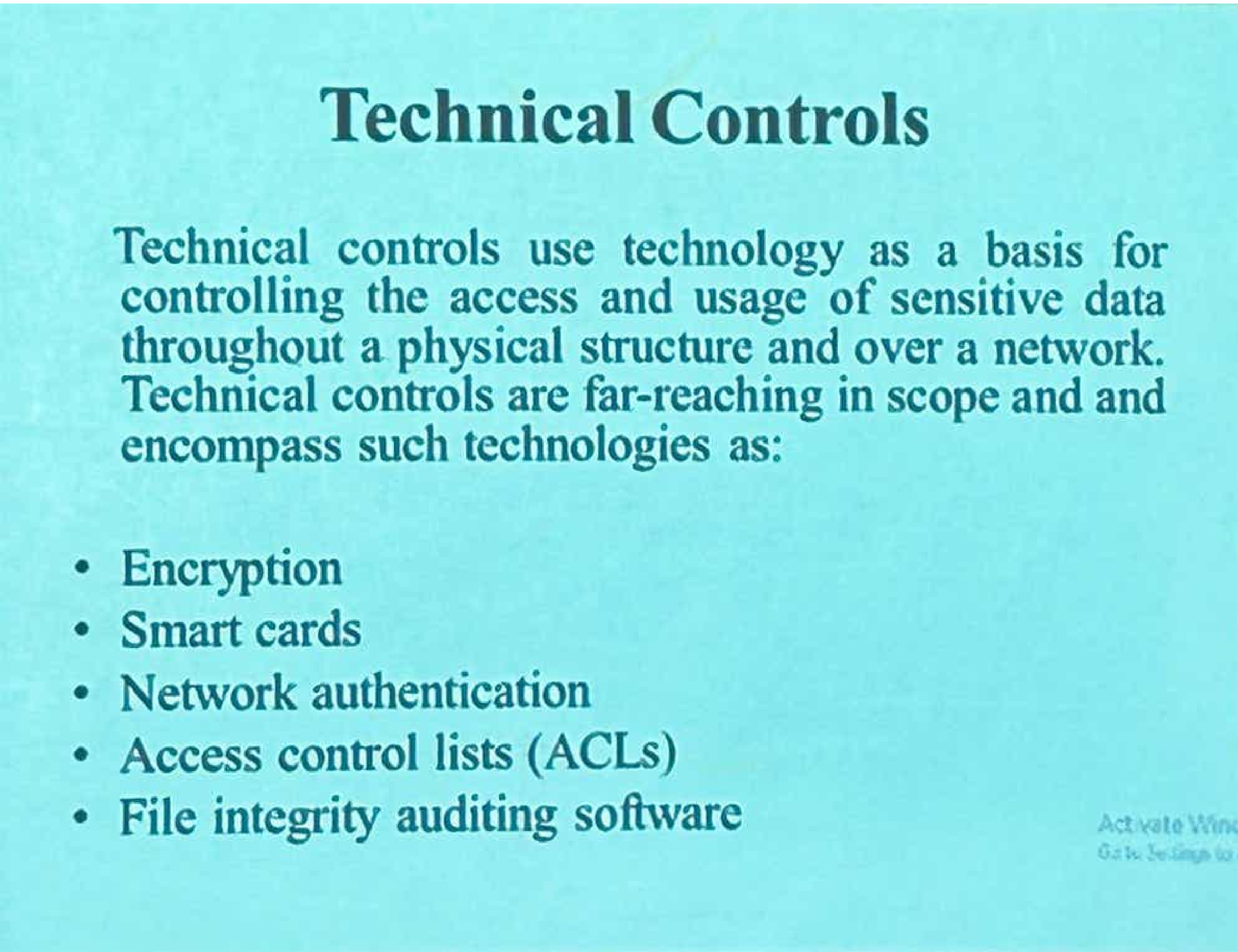


Threats to Server Security

Server security is as important as network security because servers often hold a great deal of an organization's vital information. If a server is compromised, all of its contents may become available for the cracker to steal or manipulate at will.

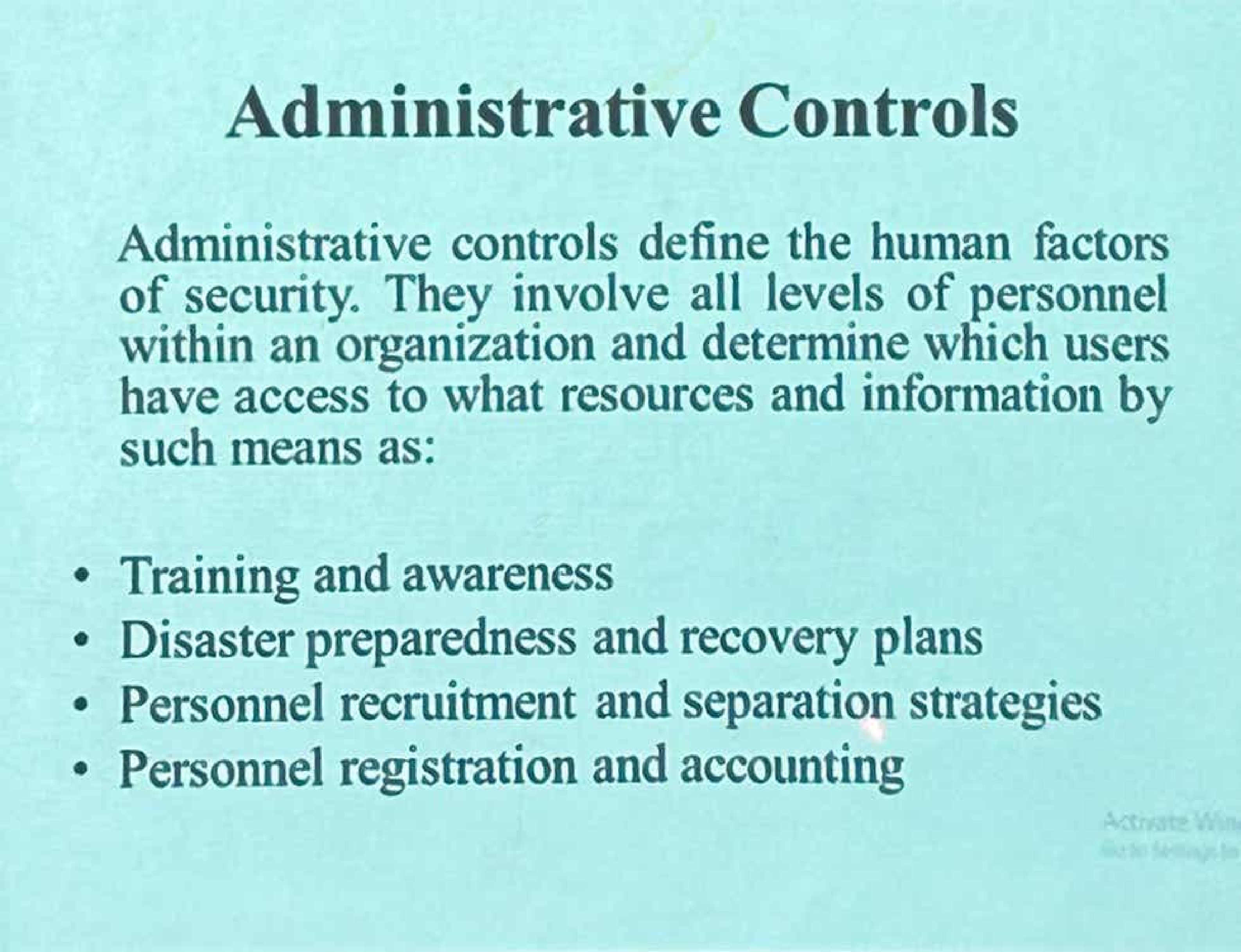
- Unused Services and Open Ports
- Unpatched Services
- Inattentive Administration
- Inherently Insecure Services



Technical Controls

Technical controls use technology as a basis for controlling the access and usage of sensitive data throughout a physical structure and over a network. Technical controls are far-reaching in scope and and encompass such technologies as:

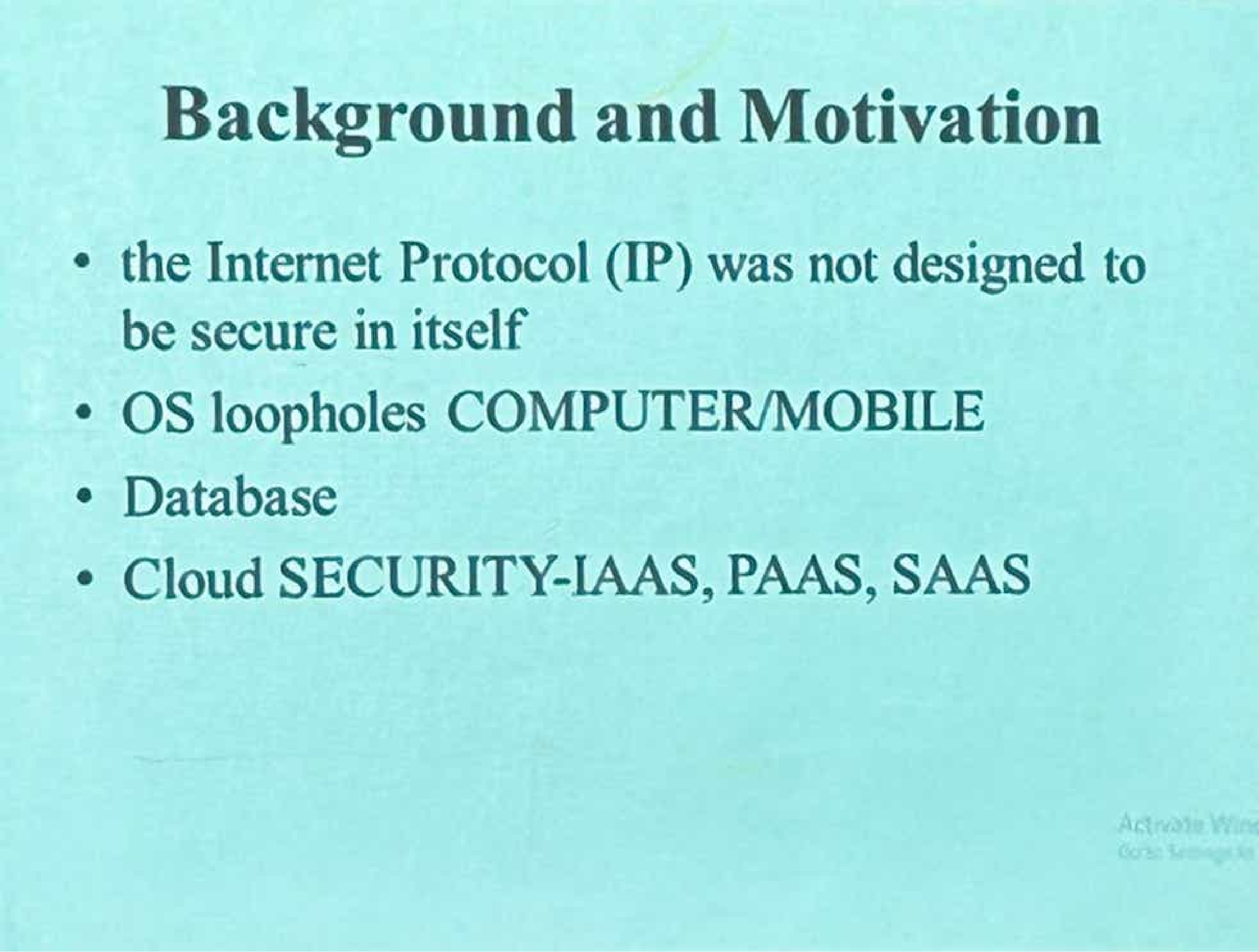
- Encryption
- Smart cards
- Network authentication
- Access control lists (ACLs)
- File integrity auditing software



Administrative Controls

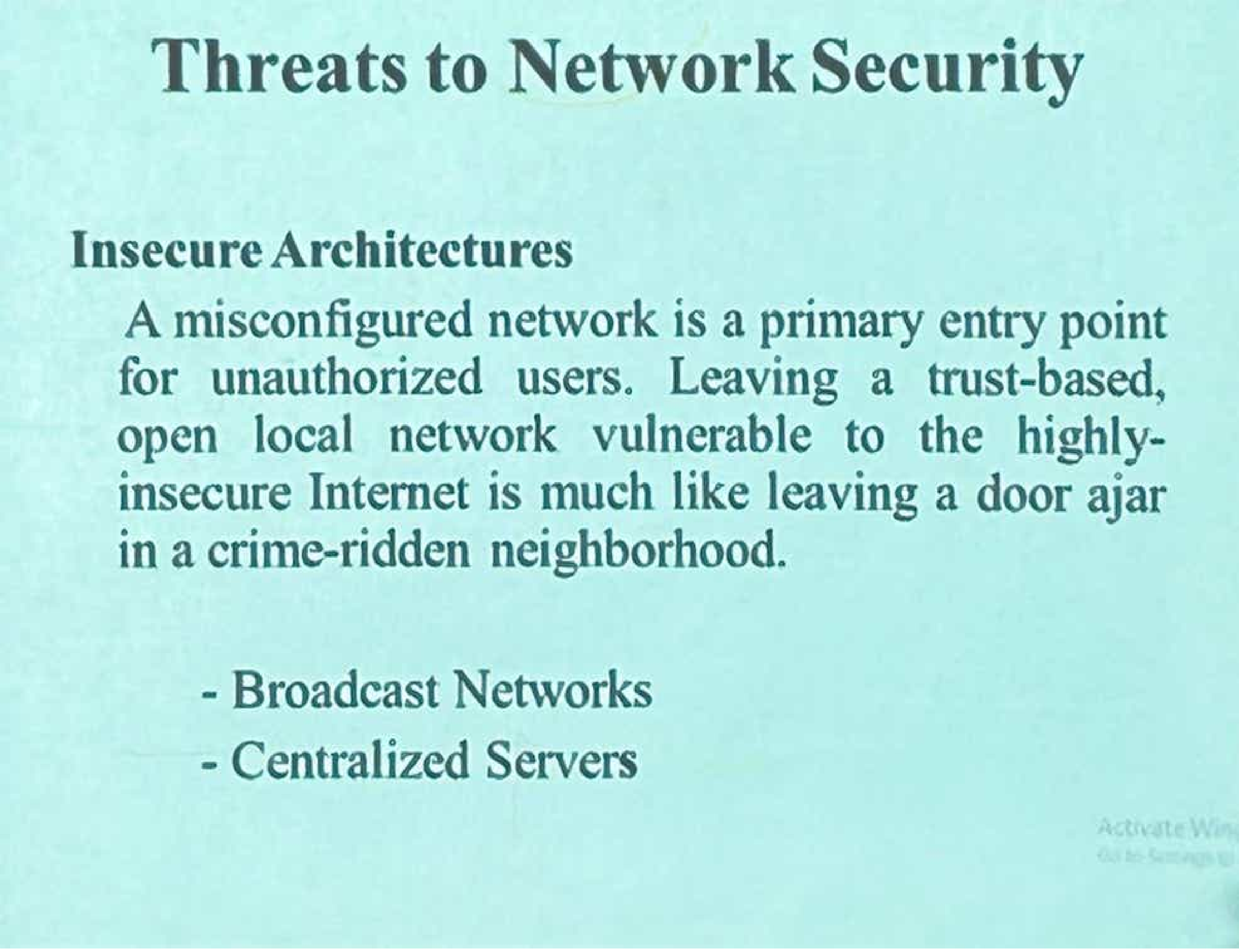
Administrative controls define the human factors of security. They involve all levels of personnel within an organization and determine which users have access to what resources and information by such means as:

- Training and awareness
- Disaster preparedness and recovery plans
- Personnel recruitment and separation strategies
- Personnel registration and accounting



Background and Motivation

- the Internet Protocol (IP) was not designed to be secure in itself
- OS loopholes COMPUTER/MOBILE
- Database
- Cloud SECURITY-IAAS, PAAS, SAAS

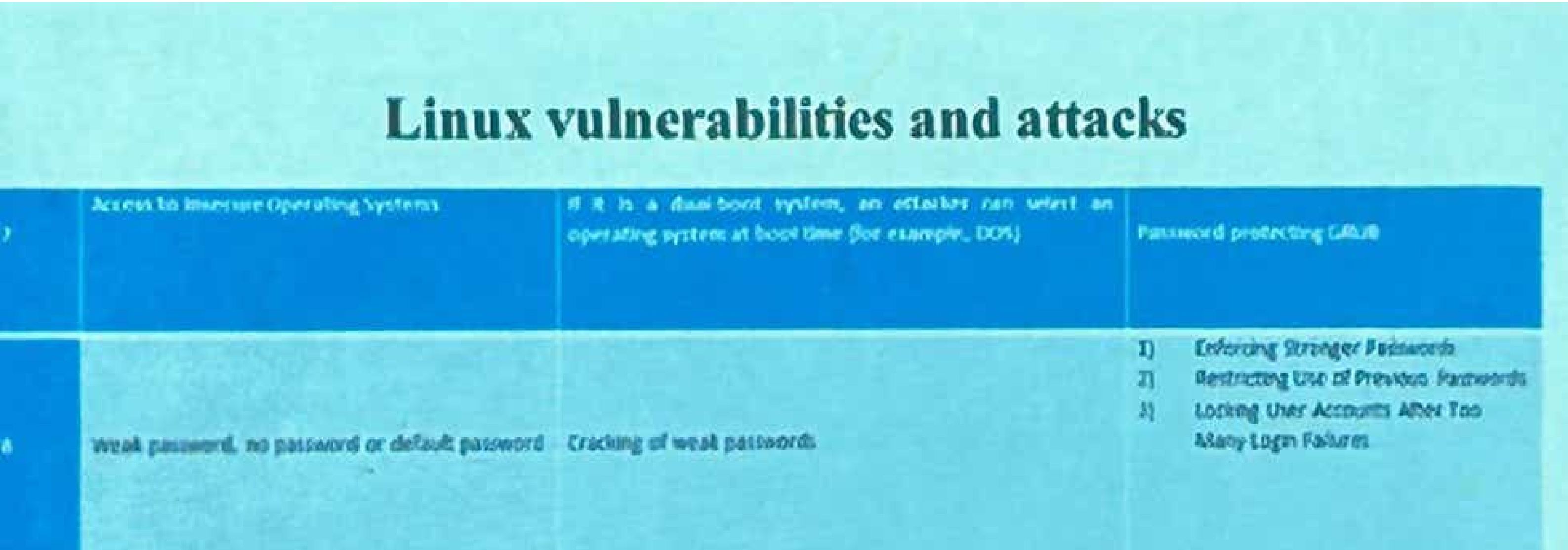


Threats to Network Security

Insecure Architectures

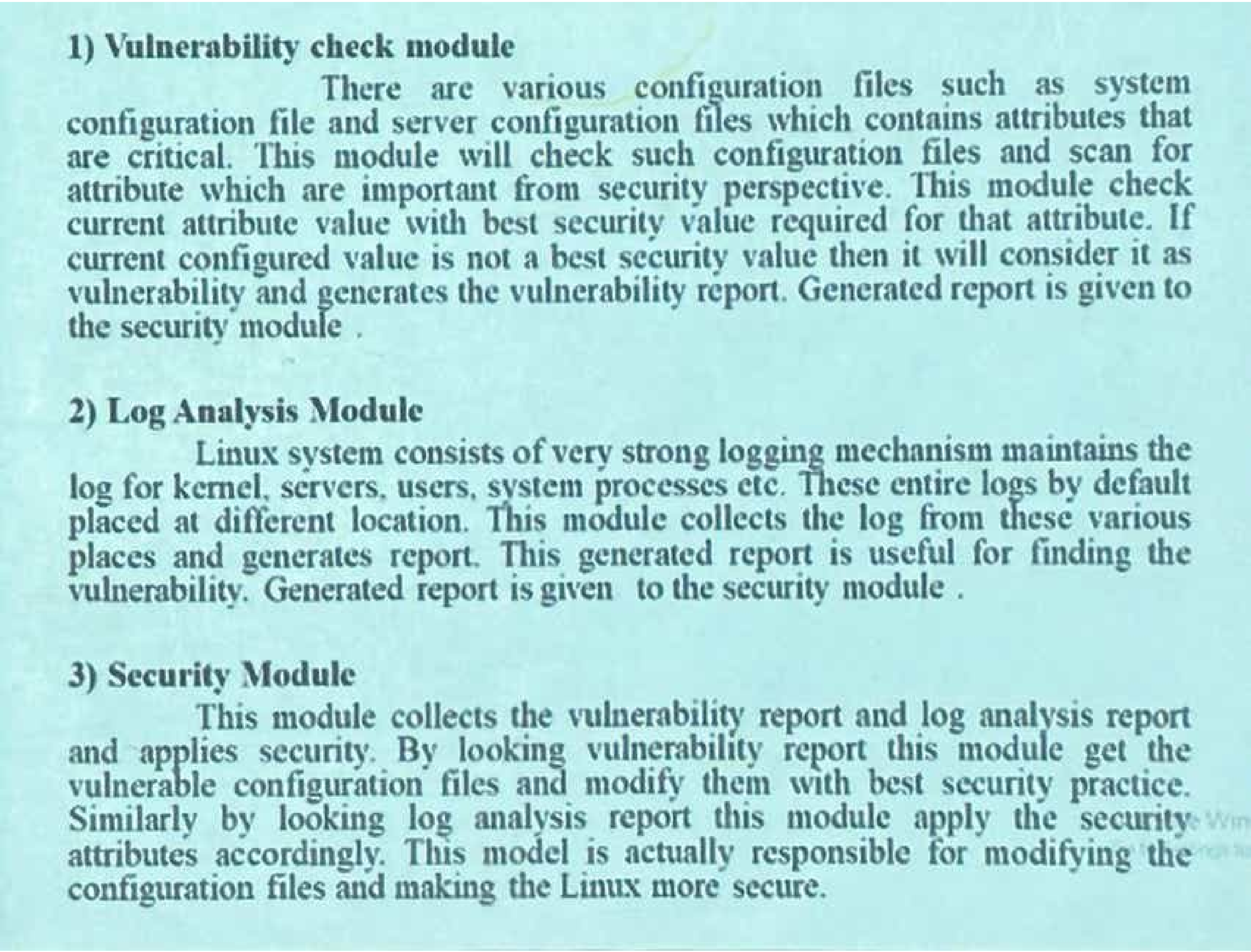
A misconfigured network is a primary entry point for unauthorized users. Leaving a trust-based, open local network vulnerable to the highly-insecure Internet is much like leaving a door ajar in a crime-ridden neighborhood.

- Broadcast Networks
- Centralized Servers



Linux vulnerabilities and attacks

7	Access to Insecure Operating Systems	If it is a dual-boot system, an attacker can select an operating system at boot time (for example, DOS)	Password protecting GRUB
8	Weak password, no password or default password	Cracking of weak passwords	1) Enforcing Stronger Passwords 2) Restricting Use of Previous Passwords 3) Locking User Accounts After Too Many Login Failures
9	No password Aging	Use of Cracked password over long period of time	Apply good password Aging
10	root access to individual users	1) Machine Misconfiguration 2) Running Insecure Services	1) Disallowing Root Access 2) Disallow Remote Root Login 3) Disabling root access via any console device (tty)
11	Allowed su command to users	Access other user data and services	Limit and block su access
12	Enabled CTRL-ALT-Delete	Unauthorized System Shut down	Disable CTRL-ALT-Delete



1) Vulnerability check module

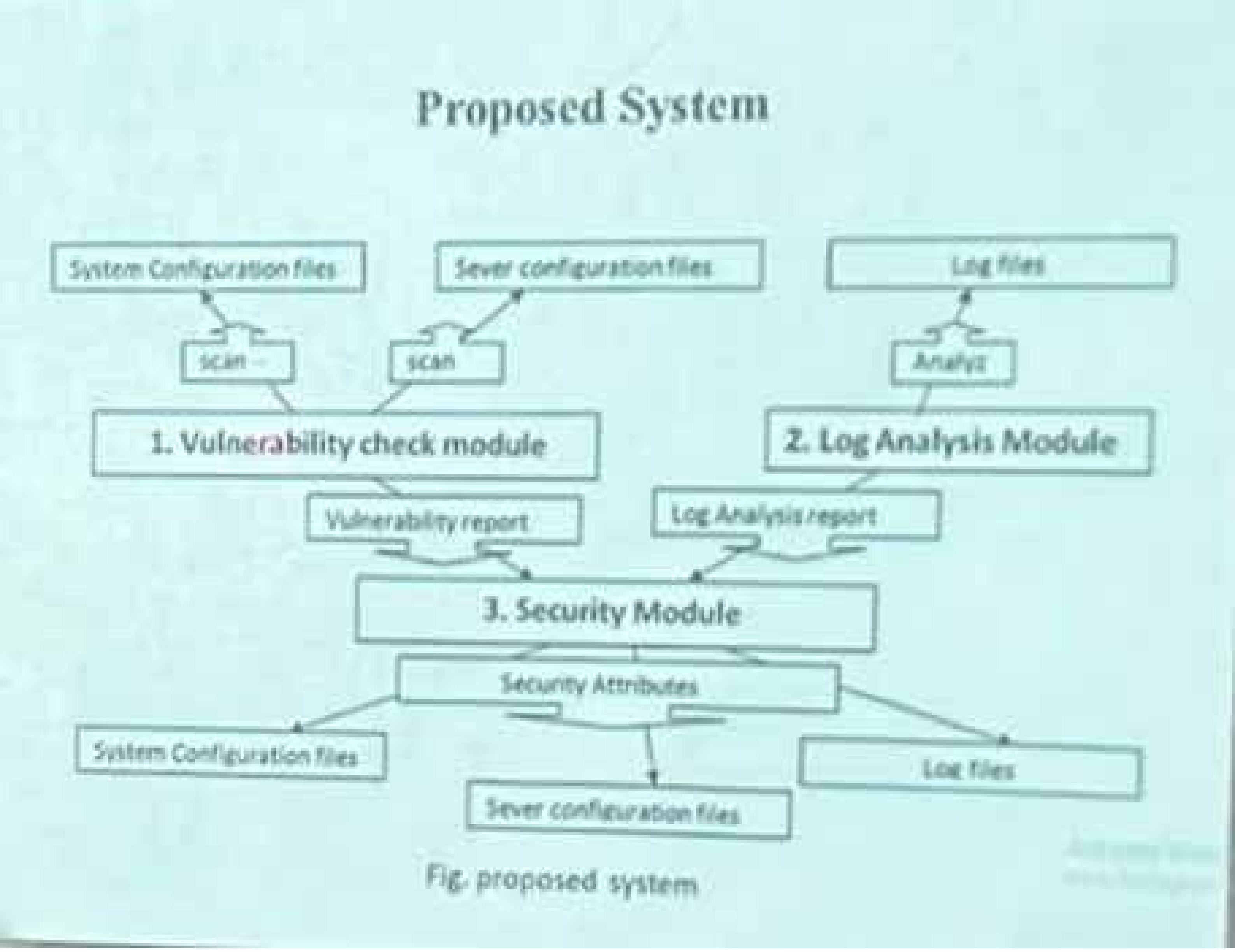
There are various configuration files such as system configuration file and server configuration files which contains attributes that are critical. This module will check such configuration files and scan for attribute which are important from security perspective. This module check current attribute value with best security value required for that attribute. If current configured value is not a best security value then it will consider it as vulnerability and generates the vulnerability report. Generated report is given to the security module .

2) Log Analysis Module

Linux system consists of very strong logging mechanism maintains the log for kernel, servers, users, system processes etc. These entire logs by default placed at different location. This module collects the log from these various places and generates report. This generated report is useful for finding the vulnerability. Generated report is given to the security module .

3) Security Module

This module collects the vulnerability report and log analysis report and applies security. By looking vulnerability report this module get the vulnerable configuration files and modify them with best security practice. Similarly by looking log analysis report this module apply the security attributes accordingly. This model is actually responsible for modifying the configuration files and making the Linux more secure.



Proposed System

System Configuration files

Sever configuration files

Log files

scan

scan

Analyz

1. Vulnerability check module

2. Log Analysis Module

Vulnerability report

Log Analysis report

3. Security Module

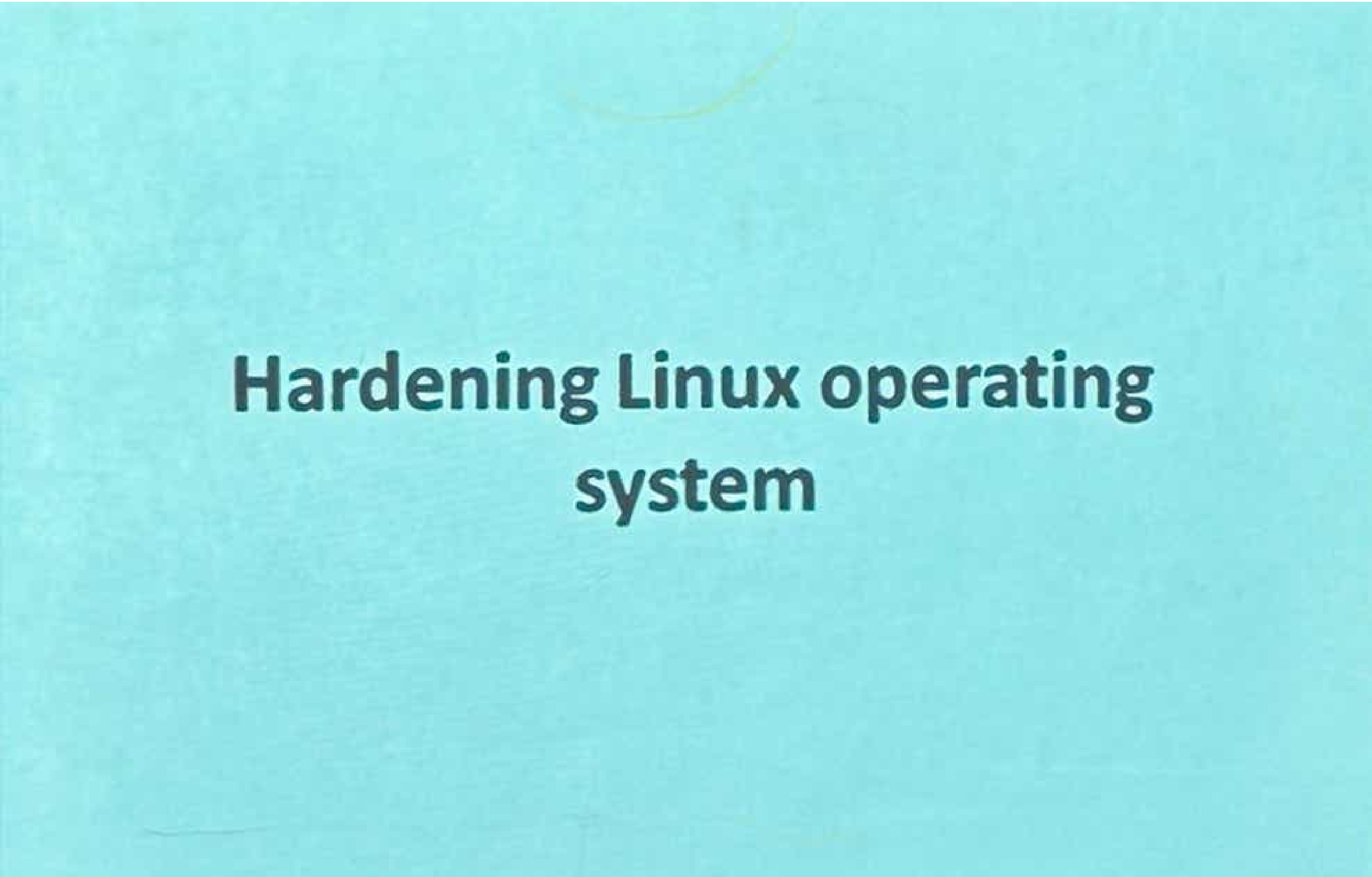
Security Attributes

System Configuration files

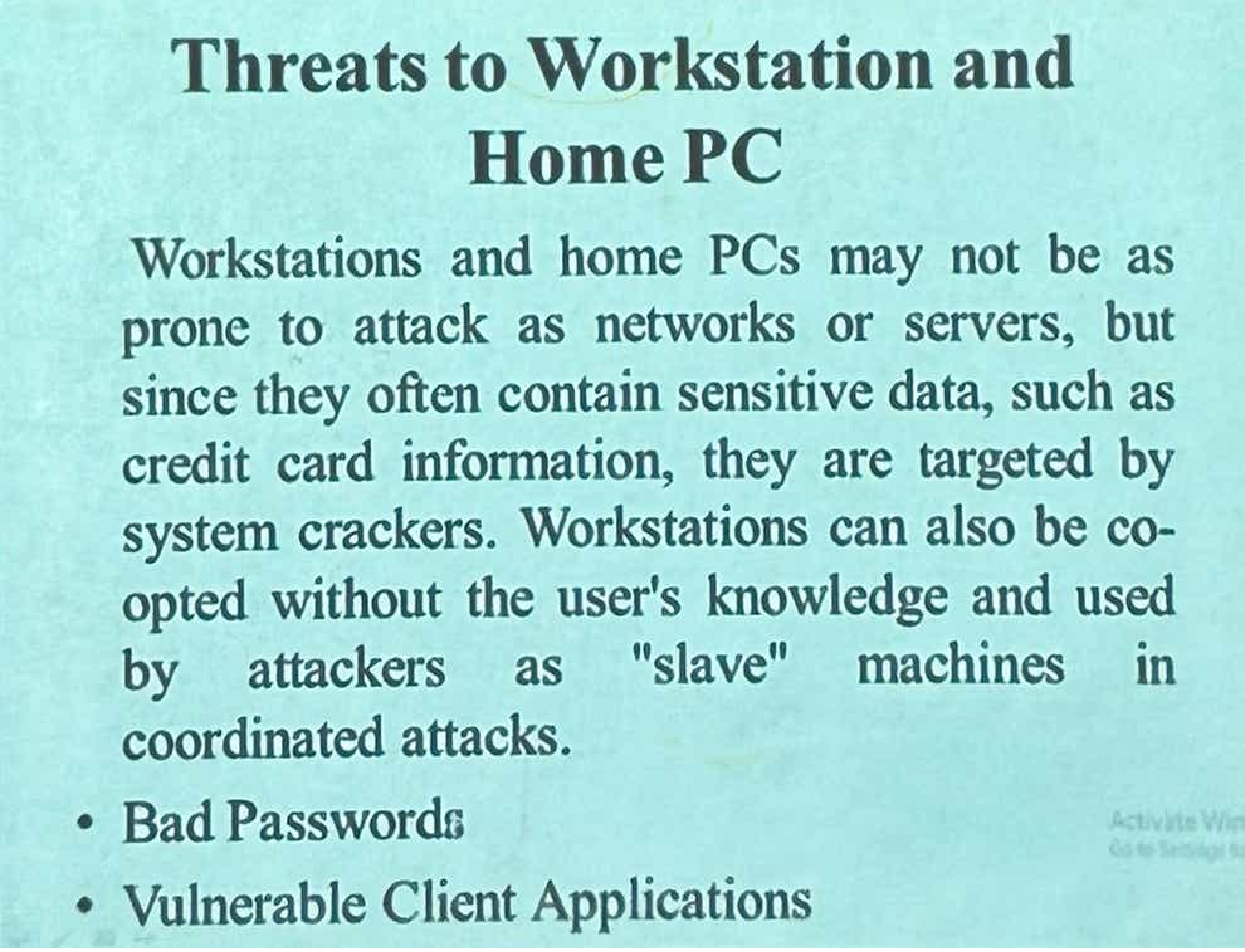
Sever configuration files

Log files

Fig. proposed system



Hardening Linux operating system



Threats to Workstation and Home PC

Workstations and home PCs may not be as prone to attack as networks or servers, but since they often contain sensitive data, such as credit card information, they are targeted by system crackers. Workstations can also be co-opted without the user's knowledge and used by attackers as "slave" machines in coordinated attacks.

- Bad Passwords
- Vulnerable Client Applications

- Art of attack
  1. form fields
  2. web page link
  3. in URL type script

0/11/23
Thursday. Linux Security.

* DB sec
  - Access control
  - Sec views – DB sec (by command access of tables & att)
  - auth & author
  - A.C. by SQL model
  - privileges & authorizat^n – diff models
  - A.C. by DAC, MAC, RBAC or their combinat^n

M

- security control = physical, technical, administrative.

- Physical control
  picture IDs
  locked & dead bolted steel doors
  security guards
  mot^n or thermal alarm sys
  closed-circuit surveillance cameras

- Technical cont.
  - encrypt^n
  - Smart card
  - networ authenticat^n
  - ACL
  - file integrity
  auditing s/w.

10M

Hardening Linux OS.

Q. What are tele vulner., attacks & defense mech.

- linux vulnerabilities & attacks

vulnerability	attacks	countermeasures
4. NO BIOS password	stealing/changing data using a bootable linux CD	Give BIOS passw
5 single user mode access	access as root user without passw.	passw. protecting BIOS
6. Access to the GRUB console GRUB is boot loader program on linux sys.	change its config or to gather info using the cat command	passw protecting GRUB.
1. No seperate partn for /boot, /home, /tmp & /var/tmp	sys. crash & data loss	create seperate partn for /boot, /home, /tmp, & /var/tmp
2. unnecessary s/w	s/w vulnerability attack	install min. s/w
3. malicious altered package	sys. instability, sys crash & data loss. data still	install signed packages.
7. access to insecure OS	if it is dual-boot syst, an attacker can select an OS at boot time. (eg. DOS)	passw. protecting GRUB 1. enforcing stronger passw 2. restricting use of previous pass 3. locking user acount after too many login

		precu
8. weak pass, no pass, default pass	cracking of weak pass	1. ____ 2. ____ 3 ____
9. no pass. aging	use of cracked pass over long period of time	apply good pass aging
). root access to indivi users	1. machine misconfig. 2. running insecure servi	1. disallowing ro ac 2. disallow remo root login 3. disabling roo access via an console devic
1. allowed su command to users	access other user data & services	limit & block su access
2. enabled CTRL-ALT-delete	unauthorized sys down	shut CTRL-AL -delete

- administrative cont.
  - training & awareness
  - disaster preparedness & recovery plan
  - personnel recruitment & seperatⁿ strate
  - personnel registratⁿ & accounting

- Background & motivatⁿ
  - IP was not designed to be secure itsel
  - OS loopholes - computer / mobile
  - db
  - cloud security - IAAS, PAAS, SAAS

Routers,
all n/w devices

system programs
os, dbms, browser

OWASP top 10
attack, DB sec

- Threat of n/w sec.
- Insecure Architech.
  - A misconfigured n/w is primary entry point for unauthorized users. leaving a trust-based open local n/w.
  - broadcast n/w
  - centralized servers

- Threats to server security
  - unused services & open ports
  - unpatch services
  - inattentive administratⁿ
  - inherently insecure services

- Thread to workstatⁿ & Home PC
  - Bad password
  - vulnerable client applⁿ