

Agenda

3 lectures →

1 Security & maintenance

2 Virtualisation I.

3 Virtualisation

Culminate by

Submitting a design of your

System Overview
diagram →

DISTRIBUTED SYSTEM with security applied

For Today

Start with Security
→

Optional - Linux
Intro

Information :-

- 1 Disrupting resources
- 2 Communication
- 3 Interfaces
- 4 Data

CIA friend.

Confidentiality - limit access to authorized.
encryption, access control, identity control.

I - Integrity - Correctness of data
Integrity check, Backup

A - Availability - Info is available when & where
needed & required.

Denial Service - DOS

physical protection to DDOS.

Access Control →
either by somebody. / Misfeasor
Somebody who has

Masquerades that doesn't have access



access and elevate his access

difficult to detect

System adminis -

Social → secret! masqueraded,

Data transportation →

passive → eavesdropping - NIC - promiscuous mode

active → man in middle.

bot false.

Source IP is spoof \rightarrow \Rightarrow reflection attack.

NAT - changing the values.

Resource Management.

Managing \rightarrow Server, VM, Infrastructure.

Monitor \rightarrow extra \rightarrow 2gb \rightarrow 128 gb.

open

Data Security \rightarrow extensive.

Data Manage.

Summary
Data distribution
Data Sourcing
Data Storage

20 min

Back at
9:00

Protect →

Information

protect us

Firewalls.

→ TCP/IP

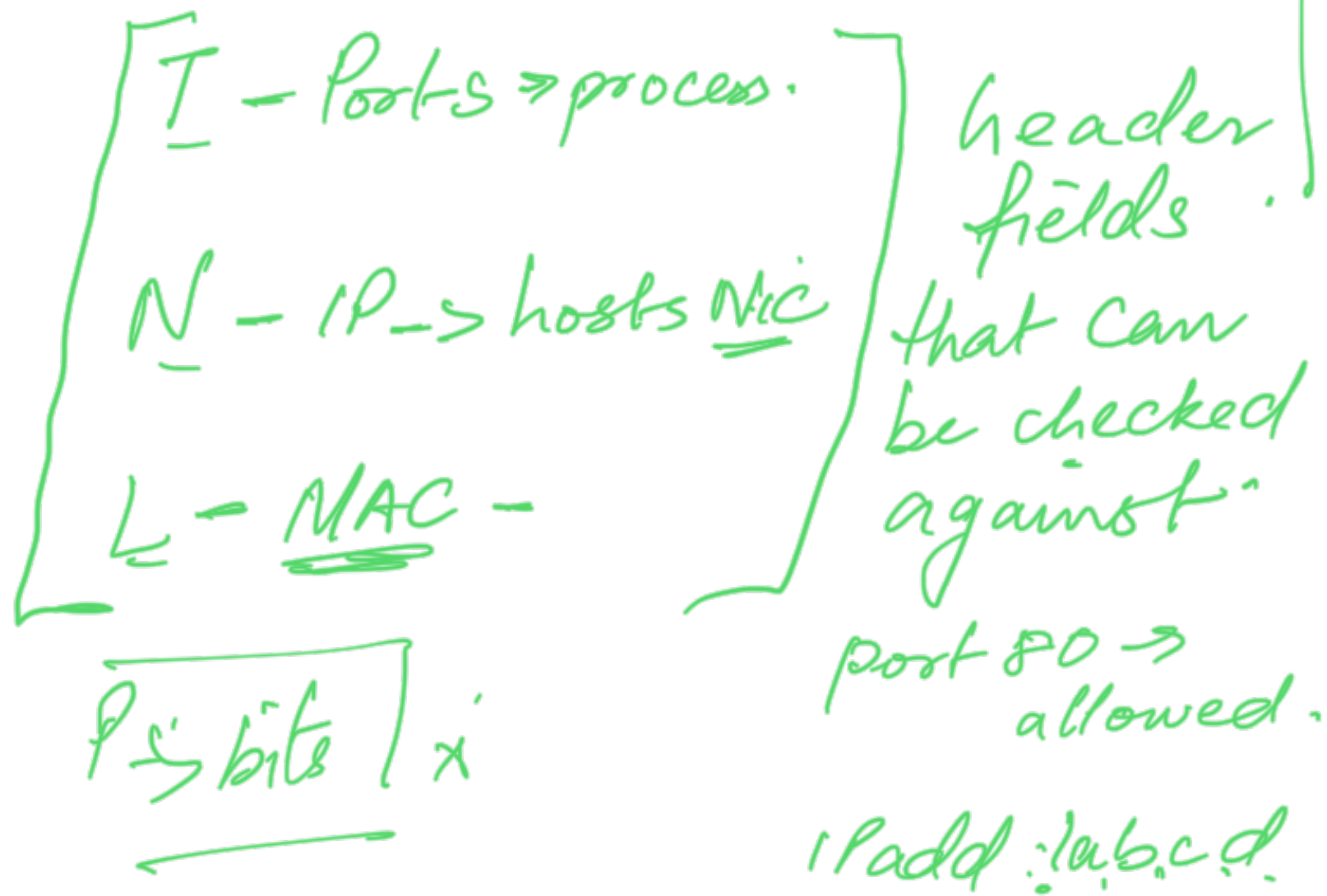
Expose our
vulnerabilities

→

map

protect

A - Proxy server, WAF



netstat

nikto \rightarrow

extensur \rightarrow http(web server) analyser with over 3000 attacks for apache, nginx

Online DDoS

~~SSL~~ Qualys

SSL Certificate

Routers

UFW \rightarrow crappy sol to iptables

IPTABLES \rightarrow Change values headers

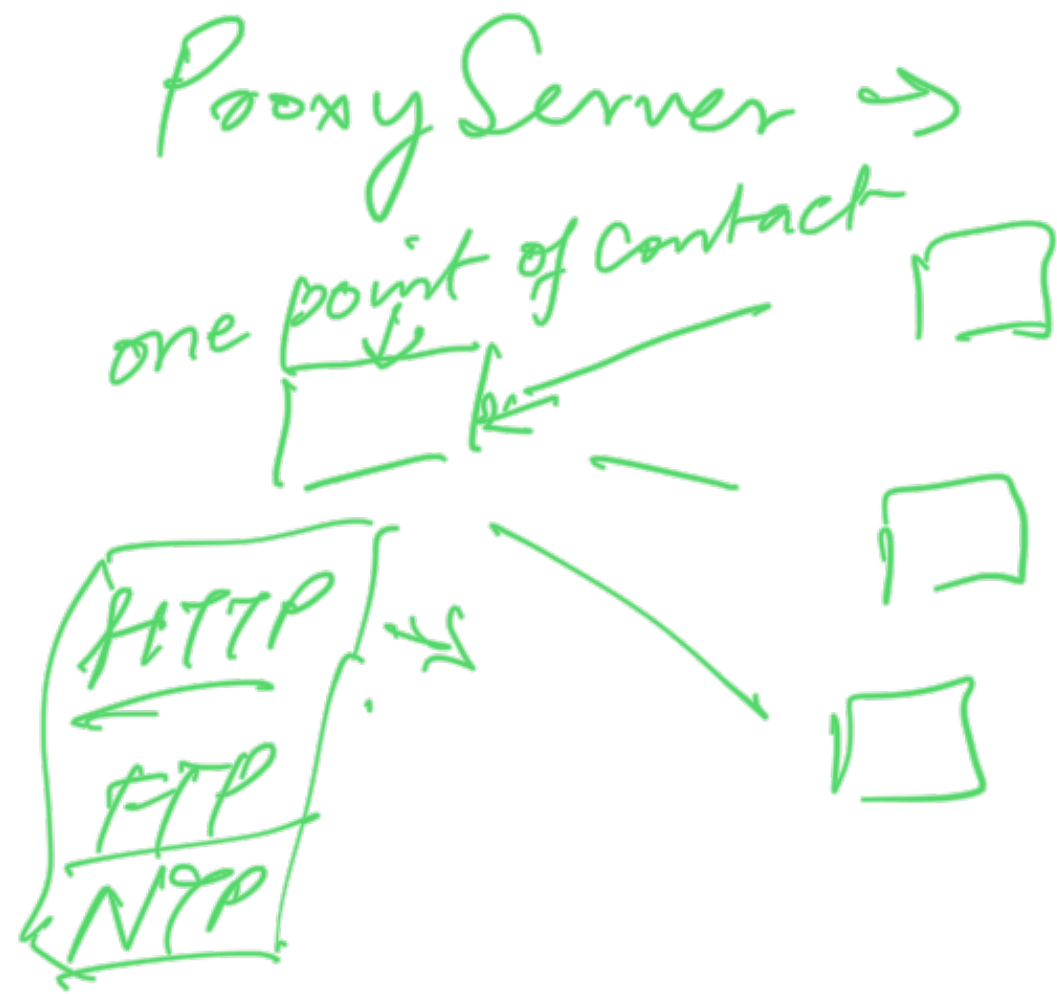
netfilter

all packet \leftarrow ~~all~~ NIC

x iptables

Geoblocking
[Nordic] ←

China, South America



Authentication → Second level.

DOS protection → TCP synflood
Reflection Attack

Limit what traffic goes out
of the server,

WAF - Web Application Firewall

Reverse proxy ← Internet



HTTP → what version
which method
content

HTTP in real time
monitor

log →

block.

and patch for vulnerability
WAF ←


application →

Mod Security Architecture

open https://www.google.com

SSL \rightarrow let's encrypt
apache

SSH \Rightarrow remote access,
public key.

bypass \Rightarrow tunnelling.
8080 \Rightarrow 22 \Rightarrow 

Host protection:

Log \rightarrow what is

happening

summarize log

log level →

Logwatch → used sudo
ssh attempt,
nginx,

Via email,

Log check

Host IDS .

Filesystem → Snapshot
integrity

Policy → which files to monitor
how they should change
read / -
→ increase.

log → increase ↵

Changing filesystem

email →

tripwire
AIDE

fail2ban

ip address.

Ssh
nginx

Backup →

rsync

webdav

Sftp

Monitor

Prometheus
Grafana
Graphite

