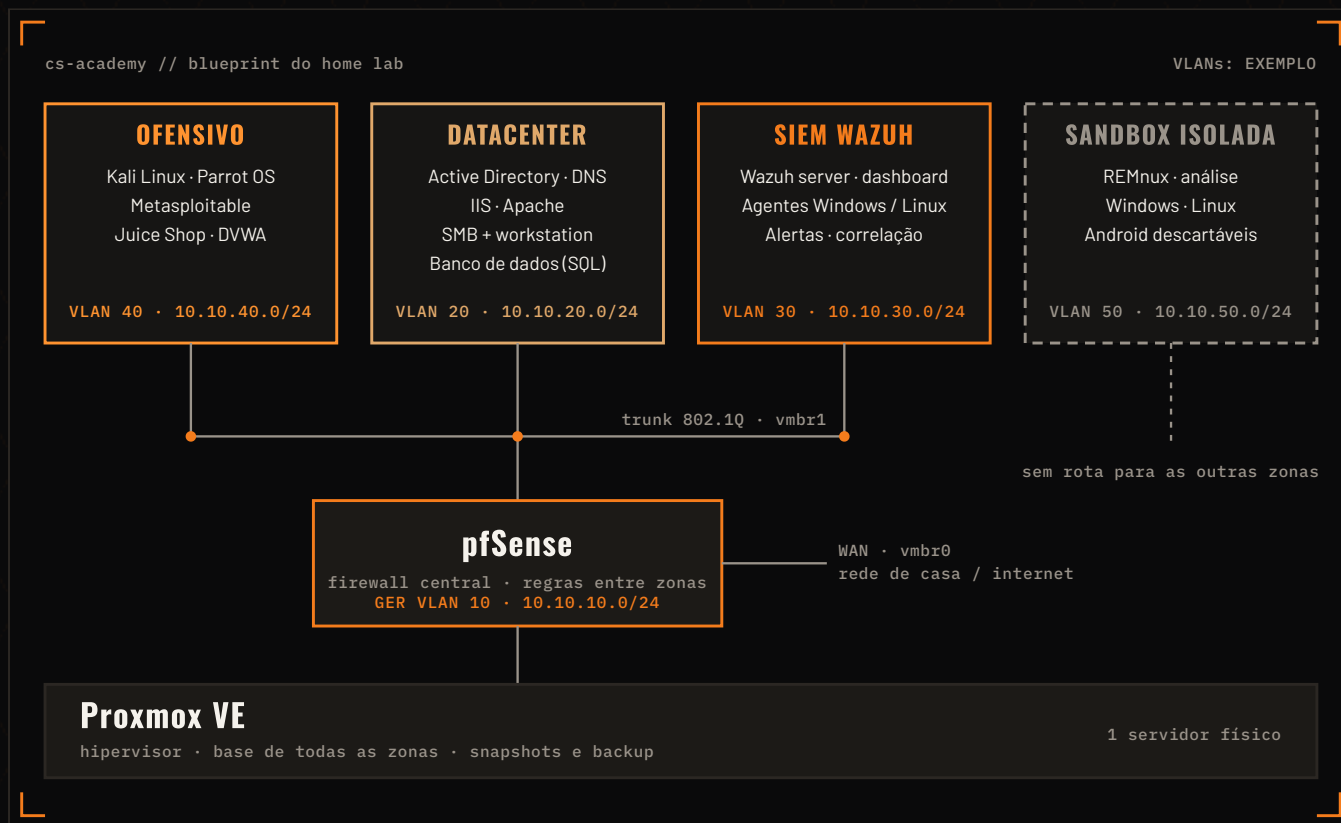


BLUEPRINT DO HOME LAB DE CIBERSEGURANÇA

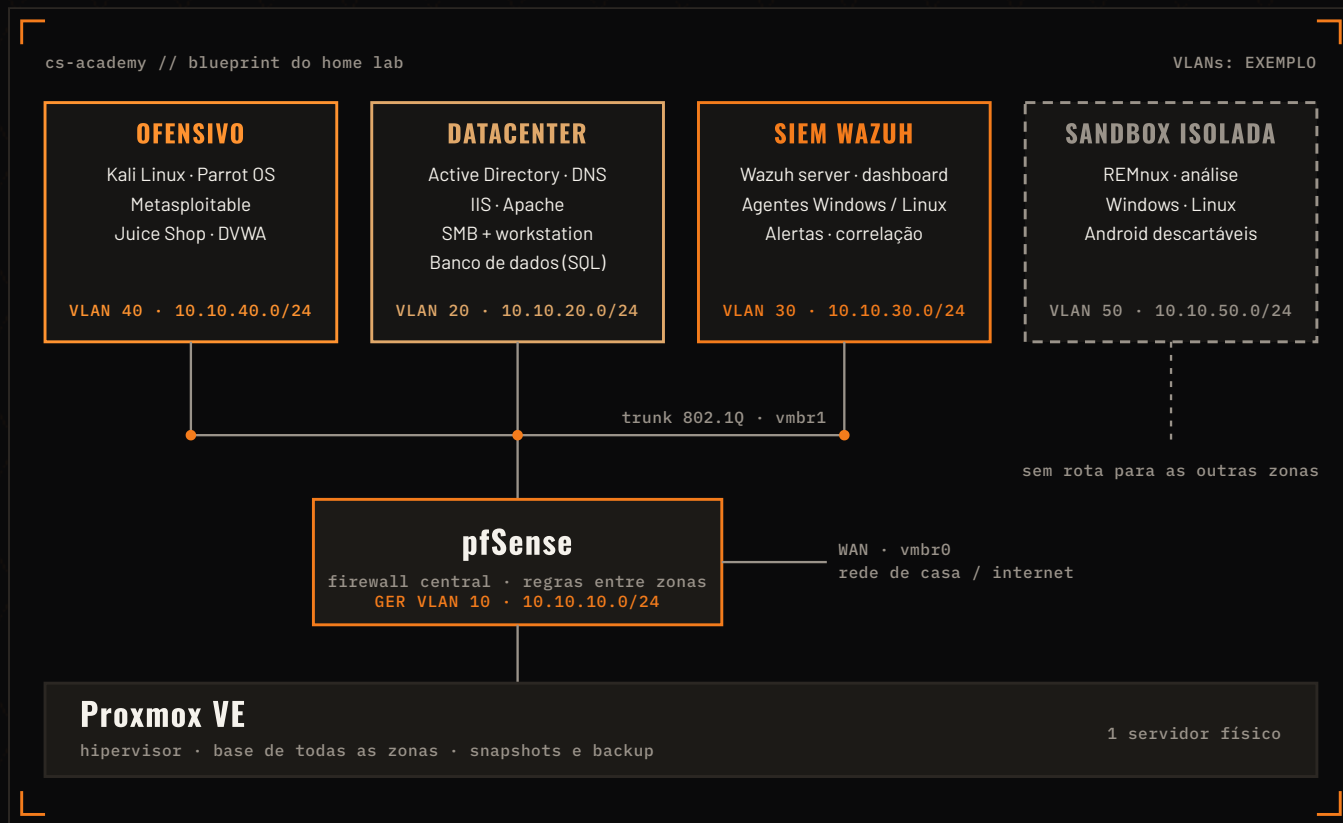
O desenho de um laboratório que simula um SOC de verdade: seis zonas, a rede que as separa, o hardware que isso exige e a ordem certa de montagem.



AS 6 ZONAS

UM HIPERVISOR, UM FIREWALL NO CENTRO

Você não vai ter dez computadores. Vai ter um, rodando dezenas de máquinas virtuais. Toda comunicação entre as zonas passa pelo pfSense, por regras que você escreve. Se o Kali enxerga o Active Directory sem passar por lugar nenhum, você não está simulando nada: está só numa LAN.



BASE PROXMOX

Hipervisor gratuito: VMs, containers, templates, snapshots e backup.

OFENSIVO

Kali e Parrot, mais alvos feitos para apanhar: Metasploitable, Juice Shop e DVWA.

SIEM WAZUH

Logs de todas as máquinas num painel: você vê o ataque acontecendo.

PFSense NO CENTRO

Firewall central: DHCP, DNS, regras, NAT e VPN entre as zonas.

DATACENTER

Rede de empresa comum: AD, IIS, Apache, SMB + workstation e banco de dados.

SANDBOX ISOLADA

Windows, Linux e Android descartáveis + REMnux, numa rede que não fala com nada.

PLANO DE VLANS E IPS

CADA ZONA NA SUA REDE (EXEMPLO)

EXEMPLO Numeração ilustrativa para você adaptar.

ZONAS, VLANS E FAIXAS · EXEMPLO

ZONA	VLAN	FAIXA (EXEMPLO)	GATEWAY	FUNÇÃO
WAN	—	Rede de casa (DHCP do roteador)	Roteador	Saída do pfSense para a internet (vmbr0)
GERÊNCIA	10	10.10.10.0/24	10.10.10.1	Interface web do Proxmox e do pfSense
DATACENTER	20	10.10.20.0/24	10.10.20.1	AD/DNS, IIS, Apache, SMB, SQL, workstation
SIEM	30	10.10.30.0/24	10.10.30.1	Wazuh server, indexer e dashboard
OFENSIVO	40	10.10.40.0/24	10.10.40.1	Kali, Parrot, Metasploitable, Juice Shop · DVWA
SANDBOX	50	10.10.50.0/24	sem rota	REMnux + VMs descartáveis, isoladas

O QUE PODE OU NÃO ACESSAR · REGRAS DE EXEMPLO NO PFSENSE

DE → PARA	GERÊNCIA	DATACENTER	SIEM	OFENSIVO	SANDBOX	INTERNET
GERÊNCIA	—	Sim	Sim	Sim	Só console do Proxmox	Sim
DATACENTER	Não	—	Só agentes Wazuh	Não	Não	Só atualizações
SIEM	Não	Não	—	Não	Não	Só atualizações
OFENSIVO	Não	Sim (alvo)	Só agentes Wazuh	—	Não	Sim
SANDBOX	Não	Não	Não	Não	—	Não

POR QUE ASSIM

O Ofensivo enxerga o Datacenter porque ele é o alvo realista. Os agentes Wazuh do Datacenter e do Ofensivo enviam os logs ao SIEM pelas portas 1514 e 1515 (TCP), e assim você vê os dois lados da mesa. O SIEM não precisa abrir conexão com as outras zonas: o pfSense libera a resposta. A Sandbox não fala com nada: quando você abrir um binário suspeito, ele não pode estar na mesma rede que o resto. Snapshot antes, detona, analisa, restaura.

CHECKLIST DE HARDWARE

MENOS DO QUE VOCÊ ACHA

O mito de que “precisa de servidor de rack” trava muita gente. Não precisa. Os requisitos abaixo são os do Cyber Security Home Lab Pro; o consumo por zona é **estimativa**.

SEU HARDWARE RODA? TRÊS PERFIS

PERFIL	RAM	CPU	DISCO	O QUE RODA
MÍNIMO VIÁVEL	16 GB	VT-x/AMD-V · 4 a 6 núcleos	SSD de 500 GB (estimativa)	Todas as zonas em versão enxuta, ligando as VMs aos poucos
RECOMENDADO	32 GB	VT-x/AMD-V · 6 núcleos ou mais	SSD/NVMe de 1 TB + HDD para backup (estimativa)	Laboratório completo; a sandbox liga quando você for analisar
FOLGA	64 GB	VT-x/AMD-V · 8 núcleos ou mais	NVMe de 2 TB + HDD para backup (estimativa)	Tudo ligado ao mesmo tempo, com espaço para crescer

Em todos os perfis: CPU com virtualização Intel VT-x ou AMD-V ligada na BIOS · Pendrive de 8 GB para instalar o Proxmox · Servidor, desktop ou mini-PC dedicado.

CONSUMO ESTIMADO POR ZONA

ZONA	O QUE RODA	RAM ENXUTA	RAM COMPLETA	DISCO
BASE PROXMOX	Reserva para o host do hipervisor	2 GB	2 GB	32 GB
PFSense (CENTRO)	Firewall central: DHCP, DNS, regras, NAT e VPN	1 GB	1 GB	16 GB
DATACENTER	AD, IIS, Apache, SMB + workstation, banco de dados Enxuta: AD + 1 servidor Linux	3 GB	11 GB	60-180 GB
SIEM WAZUH	Wazuh (servidor, indexer e dashboard) + agentes	4 GB	4 GB	50 GB
OFENSIVO	Kali, Parrot, Metasploitable, Juice Shop · DVWA Enxuta: Kali + Metasploitable	2,5 GB	5 GB	50-100 GB
SANDBOX ISOLADA	REMnux + Windows, Linux e Android descartáveis Enxuta: REMnux + 1 Linux	3 GB	9 GB	60-120 GB
TUDO LIGADO		15,5 GB	32 GB	

Wazuh: 4 GB é o mínimo para servidor, indexer e dashboard na mesma VM. Com 8 GB o painel fica bem mais confortável.

ANTES DE COMPRAR QUALQUER COISA

☐ Virtualização Intel VT-x ou AMD-V existe e está ligada na BIOS ☐ 6 núcleos ou mais ☐ 16 GB de RAM no mínimo, 32 GB recomendados ☐ SSD ou NVMe para as VMs + HDD para backup ☐ Pendrive de 8 GB para instalar o Proxmox

O CAMINHO CERTO

DA BIOS AO SOC

A ordem importa. Montar fora de sequência é a receita para “não sei por que não funciona”. Cada etapa depende da anterior.

01 HARDWARE E BIOS

Ligar a virtualização, organizar os discos, instalar o Proxmox.

02 PROXMOX

Primeira VM Windows, primeira VM Linux, containers e templates.

03 REDE

Entender bridge, NAT e VLAN, e criar as interfaces que vão isolar as zonas.

04 FIREWALL

Subir o pfSense, configurar DHCP/DNS e escrever as primeiras regras.

05 BACKUP E SNAPSHOT

Antes de construir o ambiente grande, saber como voltar atrás.

06 O DATACENTER

Active Directory, servidores, workstations.

07 O MONITORAMENTO

Wazuh, agentes nas máquinas, primeiros alertas.

08 SANDBOX E ARSENAL OFENSIVO

As zonas isoladas e as estações de ataque.

Pular a parte de rede e firewall e ir direto para “instalar o AD” é exatamente onde a maioria empaca.

ANTES DE COMEÇAR

OS ERROS QUE FAZEM A MAIORIA **DESISTIR**

REDE ÚNICA. Tudo se enxergando. Sem segmentação, sem aprendizado de verdade.

SEM SNAPSHOT. Você quebra o domínio num teste e perde um fim de semana remontando.

DATACENTER CEDO DEMAIS. Sobe o AD antes de ter rede e firewall, e nada conversa.

SANDBOX NA REDE PRINCIPAL. Um dia isso vira um problema de verdade.

SEM MONITORAMENTO. Você ataca, mas nunca vê o outro lado: perde metade do valor do lab.

PRATIQUE SÓ EM AMBIENTE PRÓPRIO OU AUTORIZADO

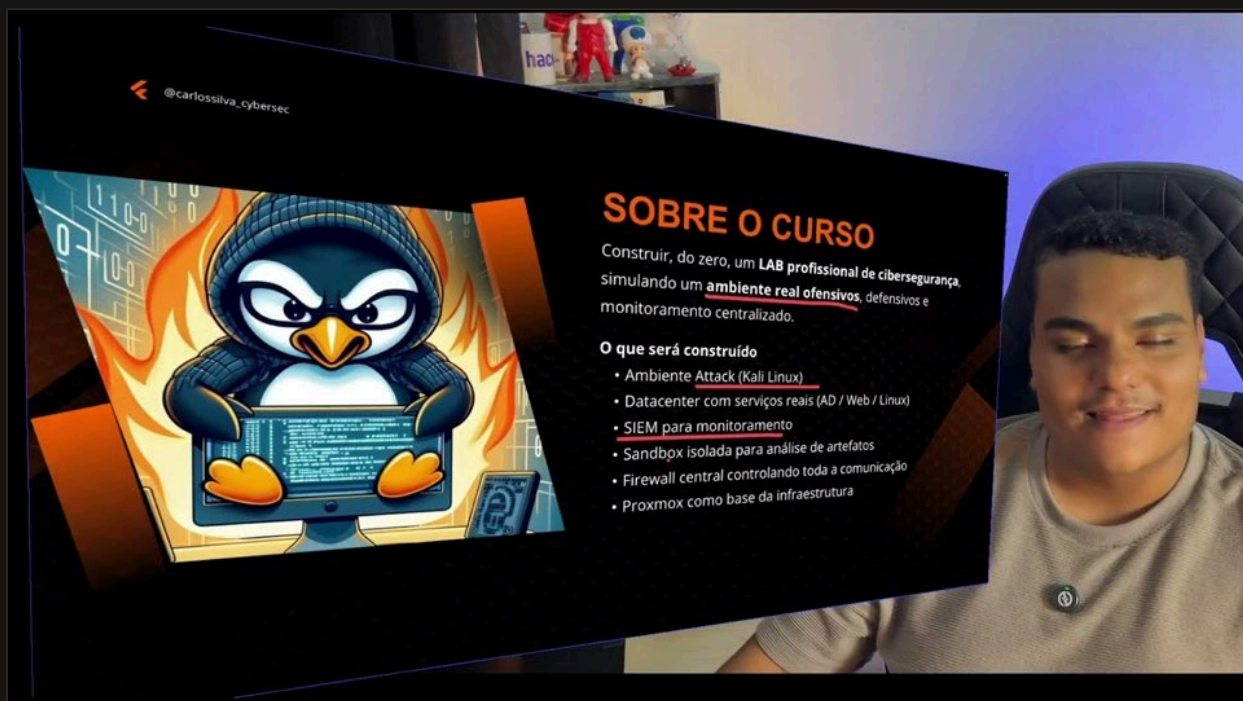
Este material é educacional. Use as técnicas de ataque apenas no seu laboratório ou em sistemas onde você tem autorização por escrito. Invadir ou testar sistemas de terceiros sem autorização pode ser crime (Lei 12.737/2012) e causar dano real.

Amostras de malware só dentro da sandbox isolada, com snapshot, e nunca na rede da sua casa.

DO DESENHO AO LABORATÓRIO

ASSISTA À AULA 1

Na primeira aula do Cyber Security Home Lab Pro, o Carlos apresenta o treinamento, mostra a arquitetura completa do laboratório e explica exatamente o que você precisa para acompanhar. É aberta, sem cadastro.



csacademysecurity.com.br/cursos/home-lab-pro/#aula1

CYBER SECURITY HOME LAB PRO

CONSTRUA ESTE LAB, PASSO A PASSO

9 módulos e 51 aulas práticas: da BIOS e do Proxmox ao Active Directory, SIEM com Wazuh, sandbox e estações ofensivas. Ferramentas gratuitas.

CONHECER O CURSO