CYBER CITY BLUEPRINTS // AULA 01

O QUE É UMA REDE E POR QUE ELA IMPORTA PARA A CIBERSEGURANÇA?

UNIVERSIDADE FEDERAL DE SERGIPE | CYLOCK — LIGA ACADÊMICA DE CIBERSEGURANÇA

SYSTEM ARCHITECTURE METAPHORS & RISKS | SHEET NO. 01/16 | SCALE: SCHEMATIC

A JORNADA DE UM CLIQUE: POR ONDE PASSAM SEUS DADOS?

A METÁFORA DO CIDADÃO EM TRÂNSITO

Imagine a seguinte situação diária:

“Quando você abre um site no seu celular, por quantos equipamentos físicos seus dados passam antes de chegar ao servidor?”

No Cyber City Blueprint, cada dado é como um cidadão viajando de sua residência local para um arranha-céu na nuvem.

1. DISPOSITIVO FINAL (HOST)

Seu celular gera a requisição de rede e a transmite via ondas de rádio (Wi-Fi).

2. PONTO DE ACESSO (ACCESS POINT)

Recebe o sinal sem fio e o injeta na infraestrutura física cabeada da rede local.

3. SWITCH DE REDE LOCAL (LAN)

Direciona os pacotes de dados dentro do seu ambiente local até encontrar a saída.

4. ROTEADOR / GATEWAY PADRÃO

A ponte que conecta sua casa ao provedor de Internet e resolve para onde enviar os dados.

5. SERVIDOR DE DESTINO

O destino final na nuvem que fornece o recurso ou página solicitada.

PROJECT: CYLOCK NETWORKS | DWG NO: A1-SH-02

SYSTEM DESIGN: CYBER CITY BLUEPRINT | SCALE: SCHEMATIC

ÁREAS DA CIBERSEGURANÇA QUE EXIGEM DOMÍNIO DE REDES

RED TEAM

Mapeia redes de alvos, identifica caminhos de ataque e executa movimentação lateral discreta.

PENTESTER

Varre portas abertas, detecta serviços expostos e explora protocolos vulneráveis.

BLUE TEAM / SOC

Monitora fluxos de rede em tempo real em busca de picos e tráfegos anômalos de invasões.

FORENSE DIGITAL

Analisa logs de roteadores e arquivos PCAP (captura de pacotes) para reconstruir ataques.

THREAT HUNTER

Caça ativamente ameaças furtivas analisando padrões em fluxos de dados de rede.

ARQUITETO DE SEG.

Desenha topologias de rede seguras, segmenta LANs e posiciona firewalls de forma resiliente.

SEG. EM NUVEM

Configura Virtual Networks (VPCs), regras de roteamento e firewalls na AWS ou Azure.

ANALISTA DE MALWARE

Isola códigos nocivos e intercepta conexões suspeitas com servidores Command & Control (C2).

SEGURANÇA DE IOT

Analisa como dispositivos inteligentes se comunicam e cria regras de isolamento na rede.

CONFORMIDADE

Audita ativos de rede (switches e roteadores) para garantir alinhamento com normas como a ISO 27001.

PROJECT: CYLOCK NETWORKS | DWG NO: A1-SH-03

SYSTEM DESIGN: CYBER CITY BLUEPRINT | SCALE: SCHEMATIC

O QUE É UMA REDE DE COMPUTADORES? (A DEFINIÇÃO)

CONCEITO CIENTÍFICO

Uma rede de computadores é um conjunto de dispositivos (como computadores, celulares, servidores e roteadores) interconectados de forma física ou lógica que conseguem se comunicar e trocar informações entre si de forma coordenada.

As conexões podem ser guiadas (cabos Ethernet, fibra óptica) ou não-guiadas (Wi-Fi, Bluetooth), unidas por um mesmo objetivo de interagir.

ANALOGIA: SISTEMA DE ESTRADAS

“Pensem na rede como um sistema de estradas.”

- Dispositivo Isolado: Uma casa no meio do nada, sem ligação nenhuma.
- Meio Físico (Estradas): Cabos de rede e Wi-Fi funcionam como o asfalto.
- Protocolo (Código de Trânsito): Regras que definem quem passa para evitar acidentes.
- Internet (A Grande Malha): A maior rede de todas: uma malha global que conecta milhares de redes menores.

QUAL O OBJETIVO PRINCIPAL DE UMA REDE? (O PROPÓSITO)

O PROPÓSITO FUNDAMENTAL É O COMPARTILHAMENTO

Desde o surgimento da ARPANET na década de 1960, conectamos máquinas não apenas para estabelecer ligações físicas, mas sim para realizar o compartilhamento otimizado de recursos em larga escala.

INFORMAÇÃO / DADOS

Compartilhamos dados em tempo real: mensagens instantâneas, arquivos compartilhados, bancos de dados corporativos, e-mails e páginas web acessadas dinamicamente.

RECURSOS FÍSICOS (HARDWARE)

Compartilhamos equipamentos físicos para reduzir custos, como vários computadores de um escritório usando a mesma impressora de rede ou um único roteador de internet.

RECURSOS LÓGICOS (PROCESSO)

Compartilhamos poder de processamento, usando servidores gigantes de banco de dados na nuvem para executar cálculos pesados que o celular não daria conta.

PROJECT: CYLOCK NETWORKS | DWG NO: A1-SH-05

SYSTEM DESIGN: CYBER CITY BLUEPRINT | SCALE: SCHEMATIC

APLICAÇÕES PRÁTICAS: REDES NO COTIDIANO

COMUNICAÇÃO & COLABORAÇÃO

SERVIÇOS EM TEMPO REAL

Plataformas como WhatsApp, e-mail, Slack e chamadas de vídeo em tempo real dependem de redes transmitindo pequenos pacotes com latência mínima.

Sem uma infraestrutura de roteamento veloz, a colaboração global moderna paralisaria instantaneamente.

ENTRETENIMENTO & STREAMING

TRANSMISSÃO SEM PAUSAS

Ao dar 'play' na Netflix ou YouTube, os arquivos não estão locais. Seu dispositivo exige que redes transmitam milhares de pacotes de dados por segundo, roteados de servidores CDN (Content Delivery Network) estrategicamente próximos.

INTERNET DAS COISAS (IOT)

MUNDO FÍSICO CONECTADO

Lâmpadas inteligentes, Smart TVs, assistentes como a Alexa e câmeras de segurança IP precisam de redes Wi-Fi locais para operar, se comunicando com a nuvem e criando novos desafios de segurança e segmentação de rede.

PROJECT: CYLOCK NETWORKS | DWG NO: A1-SH-06

SYSTEM DESIGN: CYBER CITY BLUEPRINT | SCALE: SCHEMATIC

A PONTE PARA A CIBERSEGURANÇA: ONDE TUDO SE CONECTA

A METÁFORA ESSENCIAL

“Se o objetivo de uma rede é compartilhar dados e recursos através das estradas, o objetivo da Cibersegurança é garantir que essa viagem seja segura.”
Como profissionais de segurança, não podemos apenas focar em criar estradas rápidas. Devemos proteger o veículo, a carga e os passageiros contra sabotagens, interceptações e acessos indevidos.

CONFIDENCIALIDADE

Garantir que a mensagem não seja lida por quem não deve (criptografia nos canais).

INTEGRIDADE

Garantir que ela não seja alterada ou corrompida no caminho (hashes de verificação).

DISPONIBILIDADE

Garantir que a estrada esteja sempre transitável para quem precisa (mitigação de DDoS).

RASTREABILIDADE

Saber exatamente quem enviou o quê, permitindo auditoria e logs de segurança.

PROJECT: CYLOCK NETWORKS | DWG NO: A1-SH-07

SYSTEM DESIGN: CYBER CITY BLUEPRINT | SCALE: SCHEMATIC

OBJETIVOS DE APRENDIZAGEM DA AULA

[ ] DEFINIR CONCEITOS TÉCNICOS ESSENCIAIS

Conceituar com clareza o que é rede, host, cliente, servidor, switch, roteador e gateway padrão.

[ ] MAPEAR FLUXOS DE COMUNICAÇÃO DOMÉSTICOS

Identificar e desenhar ativos físicos e fluxos básicos de troca de dados em redes residenciais ou de pequenas empresas.

[ ] GARANTIR OS PILARES DA SEGURANÇA

Relacionar cada componente de rede diretamente aos pilares de confidencialidade, integridade, disponibilidade e rastreabilidade.

[ ] APLICAR TERMINOLOGIA DE RISCO

Utilizar conceitos de Ativo, Ameaça, Vulnerabilidade, Risco e Controle para avaliar a segurança de um cenário real de IoT.

PROJECT: CYLOCK NETWORKS | DWG NO: A1-SH-08

SYSTEM DESIGN: CYBER CITY BLUEPRINT | SCALE: SCHEMATIC

VOCABULÁRIO DE REDES: A ANALOGIA DA CIDADE

TERMO TÉCNICO	METÁFORA DA CIDADE	FUNÇÃO NO BLUEPRINT DE REDE
Host	Residência / Prédio comercial	Qualquer dispositivo conectado à rede com um endereço lógico (IP) ativo.
Switch	Cruzamento ou rotatória de bairro	Conecta dispositivos dentro de uma mesma rede local (LAN). Comuta dados localmente.
Roteador	Trevo de rodovias intermunicipais	Interconecta redes logicamente diferentes e toma decisões de melhor caminho (rotas).
Access Point (AP)	Terminal de ônibus ou ponto wireless	Estende a rede local física pelo ar através de ondas de rádio bidirecionais (Wi-Fi).
Gateway Padrão	Fronteira municipal ou guarita de condomínio	A porta de saída física obrigatória que envia pacotes da rede local para a Internet.
Protocolo	Código de trânsito e semáforos	Conjunto de regras formais que estruturam e ordenam o tráfego de dados na rede.

DISPOSITIVOS DE REDE: HOSTS, CLIENTES E SERVIDORES

O CONCEITO DE HOST

DISPOSITIVO COM IP

- Definição: Qualquer dispositivo conectado à rede com endereço IP capaz de originar, receber ou rotear pacotes.
- Exemplos: Celulares, desktops, smart TVs, servidores em nuvem, impressoras e câmeras IP.
- Regra de Ouro: Todo dispositivo inteligente conectado à rede local com interface ativa é, por definição, um host.

O CLIENTE DE REDE

O SOLICITANTE DE SERVIÇOS

- Papel: O dispositivo final (ou software) que inicia a conversa solicitando dados ou recursos a outras máquinas.
- Funcionamento: Não fica aguardando conexões externas ativas. Consome dados sob demanda do usuário final.
- Exemplos: O navegador Google Chrome, o app de streaming na TV, ou o aplicativo bancário no smartphone.

O SERVIDOR DE REDE

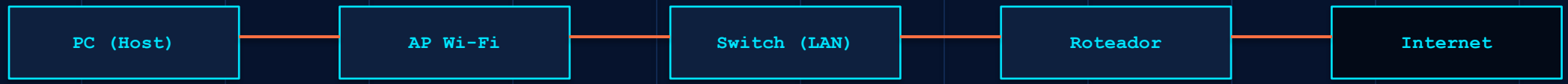
O PROVEDOR DE RECURSOS

- Papel: Máquina dedicada a escutar requisições de clientes de rede, processá-las e enviar as respostas adequadas.
- Funcionamento: Deve operar permanentemente ativo e escutando a rede em portas lógicas padronizadas.
- Exemplos: Servidores Web (hospedando sites Apache/Nginx), servidores de bancos de dados SQL e servidores de e-mail.

PROJECT: CYLOCK NETWORKS | DWG NO: A1-SH-10

SYSTEM DESIGN: CYBER CITY BLUEPRINT | SCALE: SCHEMATIC

EQUIPAMENTOS DE INTERCONEXÃO: SWITCH, ROTEADOR E AP



SWITCH (Comutador) | LAN

Conecta múltiplos dispositivos em cabo dentro da mesma rede local (LAN). Ele decodifica pacotes de dados e os direciona especificamente para a porta física do destinatário, reduzindo o tráfego desnecessário.

ROTEADOR | CONEXÃO WAN

O cérebro que decide as rotas de tráfego entre diferentes redes. Ele analisa o endereço IP de destino e decide o caminho ideal para encaminhar os dados para fora da sua rede local em direção à Internet.

ACCESS POINT (AP) | WLAN

Funciona como a extensão sem fio da rede local cabeada. Ele capta as ondas de rádio (Wi-Fi) emitidas por dispositivos móveis e as converte em sinais elétricos que trafegam na infraestrutura de cabos.

PROJECT: CYLOCK NETWORKS | DWG NO: A1-SH-11

SYSTEM DESIGN: CYBER CITY BLUEPRINT | SCALE: SCHEMATIC

O GATEWAY DE REDE: A PORTA DE SAÍDA DO SEU MUNDO

O CONCEITO DE GATEWAY

O Gateway padrão (Default Gateway) é o nó de rede encarregado de traduzir e encaminhar o tráfego interno em direção ao exterior.

Sem um gateway configurado em suas interfaces de rede, os computadores de um mesmo laboratório conseguem conversar perfeitamente entre si na LAN, mas tornam-se incapazes de carregar uma página da Internet ou alcançar servidores públicos como os do Google.

NO MUNDO REAL: REDES DOMÉSTICAS

O Roteador da sua operadora de internet (Modem Combo) é um dispositivo híbrido que executa múltiplos papéis:

- ROTEADOR + GATEWAY: Atua na Camada 3 fechando a comunicação e convertendo pacotes entre sua rede e a operadora.
- SWITCH INTEGRADO: Proporciona as portas físicas RJ-45 (LAN) na traseira para cabeamento de rede interna.
- ACCESS POINT INTEGRADO: Provê as antenas Wi-Fi internas para irradiar a conexão no ar.
- BARREIRA DE SEGURANÇA: Posição crítica para gerenciar regras básicas de firewall, acessos e monitoramento de tráfego de entrada e saída.

PROJECT: CYLOCK NETWORKS | DWG NO: A1-SH-12

SYSTEM DESIGN: CYBER CITY BLUEPRINT | SCALE: SCHEMATIC

O FLUXO DE COMUNICAÇÃO: OS 4 ELEMENTOS FUNDAMENTAIS

1. ORIGEM

O EMISSOR DE DADOS

O host físico ou aplicação lógica que inicia o fluxo de transmissão (ex: navegador web enviando requisição HTTP).

2. DESTINO

O RECEPTOR FINAL

O host final receptor dos pacotes na rede (ex: servidor web que processa a requisição e envia a resposta).

3. MEIO

O CANAL DE TRÂNSITO

O meio físico ou sinal eletromagnético de tráfego: cabos de cobre Ethernet, conexões ópticas ou ondas de rádio (Wi-Fi).

4. REGRAS

OS PROTOCOLOS

Normas formais de formatação e controle de fluxo (ex: TCP/IP, HTTP). É o que define se 'conseguiremos nos entender'.

PROJECT: CYLOCK NETWORKS | DWG NO: A1-SH-13

SYSTEM DESIGN: CYBER CITY BLUEPRINT | SCALE: SCHEMATIC

FUNDAMENTOS DE CIBERSEGURANÇA APLICADOS A REDES

ATIVO

O QUE PROTEGER

Qualquer recurso, dado ou serviço digital valioso residente na rede que a organização deve resguardar.

Ex: Banco de dados com registros de usuários.

VULNERABILIDADE

A FRAQUEZA DO SISTEMA

Falha técnica, erro de configuração ou falha operacional que permite exploração externa.

Ex: Servidores em operação com credenciais padrão.

AMEAÇA

O PERIGO EXTERNO

Agente externo, hacker, malware ou evento nocivo capaz de explorar vulnerabilidades.

Ex: Criminosos virtuais fazendo varreduras automáticas.

RISCO

A PROBABILIDADE

Chance de uma ameaça comprometer um ativo explorando uma falha real, gerando perdas.

Ex: Roubo de dados sensíveis ou colapso do serviço.

CONTROLE

AS SALVAGUARDAS

Medidas técnicas e políticas de proteção para conter ameaças e brechas.

Ex: Implantação de MFA, regras de firewall e logs de auditoria.

PROJECT: CYLOCK NETWORKS | DWG NO: A1-SH-14

SYSTEM DESIGN: CYBER CITY BLUEPRINT | SCALE: SCHEMATIC

ESTUDO DE CASO PRÁTICO: CÂMERA IP COM SENHA PADRÃO

CENÁRIO DE INFRAESTRUTURA IOT

“Uma câmera de monitoramento IP residencial é instalada conectada diretamente à Internet, operando com as credenciais padrão de fábrica (usuário: admin / senha: admin).”
Este caso clássico é um excelente modelo para exercitar o mapeamento de risco cibernético:

1. ATIVO

A Câmera IP instalada, que grava imagens físicas do ambiente interno residencial.

2. VULNERABILIDADE

Credencial original (admin/admin) mantida ativa e sem criptografia de controle de acesso.

3. AMEAÇA

Varreduras públicas automatizadas (como Shodan) buscando portas HTTP abertas na internet.

4. RISCO

Invasão e transmissão das imagens domésticas para a Web ou incorporação do host em botnets.

5. CONTROLES

Alterar credenciais de fábrica imediatamente, isolar a câmera em uma VLAN/rede IoT e criar regras de firewall no gateway.

DESAFIO COGNITIVO // COMPARTILHAMENTO

DESAFIO DE DIAGNÓSTICO DE FLUXO:

Esboce no papel o caminho aproximado de conexão que liga seu computador até os servidores de streaming da Netflix.

Após o desenho, classifique os seguintes itens no seu esquema:

✓ 3 Ativos críticos envolvidos na comunicação
✓ 1 Vulnerabilidade potencial ao longo da rota
✓ 1 Ameaça lógica à transmissão dos pacotes
✓ 2 Controles aplicáveis no gateway doméstico

CONTINUIDADE DOS ESTUDOS // INDEPENDENTE

PRÓXIMOS PASSOS: LABORATÓRIO VIRTUAL

Acesse a plataforma de aprendizado TryHackMe:

■ Módulo recomendado: 'Pre Security - Introduction to Networking'

Este laboratório ajudará você a visualizar graficamente o envio de pacotes através de firewalls, compreender o funcionamento lógico de gateways e praticar de forma segura comandos fundamentais no terminal antes do nosso próximo encontro técnico.