CYLOCK / UFS

Endereçamento de Redes Aplicado à Cibersegurança

IPv4, IPv6, MAC e CIDR na investigação de um incidente na empresa fictícia da CyLock.

IPv4 • IPv6 • MAC • SUB-REDES E CIDR

AULA DE 44 MINUTOS

Liga Acadêmica de Cibersegurança

O servidor sumiu depois da mudança de rede

09h10. A empresa dividiu uma rede /24 em sub-redes /26. Uma estação apresenta acesso parcial.

01

O que funciona

A estação A alcança a estação B e o portal interno.

02

O que falha

A estação A não alcança o servidor C após a mudança.

03

Nossa missão

Descobrir o próximo salto e conferir as evidências de enlace.

BLUE TEAM

Diagnosticar a falha

RED TEAM

Validar o escopo

FORENSE DIGITAL

Reconstruir o caminho

PERGUNTA Por que alguns destinos funcionam e outro deixou de responder?

Os endereços do nosso caso

Plano esperado após a mudança. O gateway da estação A é 10.10.10.65.

ESTAÇÃO A	10.10.10.70/26
ESTAÇÃO B	10.10.10.90/26
SERVIDOR C	10.10.10.130/26
PORTAL INTERNO	10.10.30.20/24
GATEWAY DE A	10.10.10.65/26

CONDIÇÕES DO CENÁRIO

- A e B compartilham a VLAN 110.
- C está em outra VLAN, a VLAN 120.
- As rotas e regras permitem os fluxos do caso.

CONVENÇÃO **Nos exemplos de entrega roteada, não há NAT nem proxy.**

O prefixo define o tamanho da rede

10.10.10.70/26 tem 32 bits. O /26 reserva 26 bits para a rede e deixa 6 para hosts.

IPv4

ENDEREÇO

Quatro octetos de 0 a 255.
Exemplo: 10.10.10.70

32 bits no total

/26

PREFIXO CIDR

Indica quantos bits iniciais pertencem ao prefixo da rede.

Máscara: 255.255.255.192

6 bits

PARTE DE HOST

32 − 26 = 6
2^6 = 64 endereços no bloco.

62 hosts no caso tradicional

Mais bits no prefixo significam menos endereços por sub-rede.

Em qual bloco está 10.10.10.70/26?

Máscara 255.255.255.192. No último octeto, cada bloco ocupa 64 endereços.

01	**Tamanho do bloco**	256 − 192 = 64. Os blocos começam em .0, .64, .128 e .192.
02	**Endereço de rede**	70 está entre 64 e 127. A rede é 10.10.10.64/26.
03	**Hosts utilizáveis**	10.10.10.65 até 10.10.10.126. São 62 endereços para interfaces.
04	**Broadcast IPv4**	10.10.10.127. O bloco seguinte começa em 10.10.10.128.

O gateway .65 usa um dos endereços de host. Ser o primeiro host é uma escolha do projeto.

O mesmo /24 pode virar quatro /26

Bloco de origem: 10.10.10.0/24. O prefixo também define o alcance de uma regra ou teste.

/24

UM BLOCO

Rede .0
Broadcast .255
254 hosts tradicionais

Máscara 255.255.255.0

/25

DOIS BLOCOS

Inícios .0 e .128
128 endereços por bloco
126 hosts por sub-rede

Máscara 255.255.255.128

/26

QUATRO BLOCOS

Inícios .0, .64, .128 e .192
64 endereços por bloco
62 hosts por sub-rede

Máscara 255.255.255.192

Um teste autorizado para 10.10.10.64/26 cobre .64 a .127. Um /24 amplia o escopo.

Endereços privados e especiais

Antes de investigar um IP, identifique o intervalo e o contexto da interface.

PRIVADO	10.0.0.0/8
PRIVADO	172.16.0.0/12
PRIVADO	192.168.0.0/16
LOOPBACK	127.0.0.0/8, como 127.0.0.1
LINK-LOCAL	169.254.0.0/16

LEITURA DE SEGURANÇA

- IP privado também pode aparecer em tráfego malicioso.
- IP público não garante que exista um serviço exposto.
- 169.254 pode indicar falta de configuração utilizável.

ATENÇÃO O intervalo privado 172 vai de 172.16.0.0 até 172.31.255.255.

A rota vem antes da consulta ARP

A está configurada corretamente como 10.10.10.70/26. Há uma rota padrão via 10.10.10.65.

01	**Tabela de rotas**	O sistema procura a rota correspondente com o prefixo mais específico.
02	**Destino local: .90**	A rota 10.10.10.64/26 indica entrega direta no enlace.
03	**Destino remoto: .130**	Sem outra rota específica, A usa o gateway 10.10.10.65.
04	**Resolução no enlace**	ARP procura o MAC do próximo salto escolhido: o destino local ou o gateway.

Se não houver rota aplicável, a transmissão falha. O gateway não corrige uma rota errada no host.

Entrega local: A procura o MAC de B

A quer enviar um ping para 10.10.10.90. O cache ARP começa vazio.

01	**ARP Request**	“Quem tem 10.10.10.90?” A envia para ff:ff:ff:ff:ff:ff.
02	**ARP Reply**	B responde normalmente em unicast: “.90 está no MAC 02:00:00:00:10:90”.
03	**Cache de A**	A guarda temporariamente .90 associado ao MAC 02:00:00:00:10:90.
04	**ICMP Echo**	A envia o pedido ao MAC de B. A resposta ICMP é uma etapa separada.

MAC Ethernet tem 48 bits. Pode mudar ou ser falsificado, por isso exige contexto para atribuição.

O IP aponta para C. O MAC aponta para o próximo salto

A envia para 10.10.10.130 por um roteador. Não há NAT neste exemplo.

ENLACE DE A

Primeiro quadro Ethernet



IP destino: 10.10.10.130
MAC destino: MAC do gateway .65

ENLACE DE C

Novo quadro Ethernet



IP destino: 10.10.10.130
MAC destino: MAC de C

SEM NAT

O roteador troca o quadro. Os endereços IP permanecem.

Três tabelas com funções diferentes

Um registro pode estar correto e ainda assim a comunicação falhar em outra etapa.

Rota

PREFIXO E PRÓXIMO SALTO

No host ou roteador.
Destino remoto: usar o gateway 10.10.10.65.

Pergunta: por onde enviar?

ARP

IPv4 E MAC

No host ou roteador.
10.10.10.65 associado a 02:00:00:00:10:65.

Pergunta: qual MAC usar?

MAC

MAC E PORTA DO SWITCH

No switch.
O MAC da estação A está na porta de acesso daquela VLAN.

Pergunta: por qual porta sair?

Blue Team correlaciona essas tabelas. Na perícia, uma captura remota pode mostrar o MAC do roteador.

A estação A manteve a máscara antiga

Configuração efetiva de A: 10.10.10.70/24. O plano exige /26.

O QUE A ACREDITA

Rede 10.10.10.0/24

A considera .130 local. Emite ARP por .130 na VLAN 110, onde C não está.

O QUE O PLANO EXIGE

Rede 10.10.10.64/26

C fica em outro segmento. A deve entregar o pacote ao gateway .65.

CORREÇÃO DO CASO

Aplicar o /26

Após a correção, A resolve o gateway e alcança C pelo roteador.

Uma máscara incorreta explica o acesso parcial. Esse sintoma, sozinho, não comprova um ataque.

IPv6: o prefixo continua importante

128 bits, escritos em hexadecimal. Uma interface pode ter vários endereços IPv6.

REPRESENTAÇÃO

2001:db8:10::70

Prefixo do exemplo: /64

Forma expandida:
2001:0db8:0010:0000:
0000:0000:0000:0070

2001:db8::/32 é reservado à documentação.

REGRAS DE LEITURA

Zeros podem sumir

- Zeros à esquerda de um grupo podem ser omitidos.
- :: substitui grupos consecutivos de zeros uma única vez.
- Em LANs com SLAAC, /64 é o tamanho usual do prefixo.

O número após / continua contando bits, agora em um endereço de 128 bits.

O alcance do endereço muda a investigação

A mesma interface pode participar do enlace local e de comunicações roteadas.

::1	**Loopback** O host conversa consigo mesmo. Equivalente funcional ao loopback IPv4.	Uma resposta aqui não testa o caminho físico.
fe80::/10	**Link-local** Comunicação no enlace local. Pode aparecer como endereço do roteador padrão.	Precisa de contexto de interface e fica no enlace.
Global	**Unicast global** Pode ter alcance global com rotas e política adequadas. Exemplo didático: 2001:db8:10::70.	O endereço de documentação do exemplo não circula na Internet pública.

PERGUNTA Um host com IPv4 privado pode manter comunicação IPv6 ativa?

IPv6 descobre vizinhos com ICMPv6

Neighbor Discovery usa mensagens próprias. IPv6 não usa ARP nem broadcast.

NEIGHBOR DISCOVERY

NS e NA

Neighbor Solicitation procura o vizinho. Neighbor Advertisement informa a associação de enlace.

DESCOBERTA DE ROTEADOR

RS e RA

Router Solicitation pede anúncios. Router Advertisement informa roteadores e parâmetros da rede.

PILHA DUPLA

Duas superfícies

Monitoramento e políticas precisam cobrir IPv4 e IPv6. Anúncios falsos também exigem atenção.

Bloquear todo ICMPv6 pode quebrar funções essenciais. O filtro precisa considerar o tipo de mensagem.

A turma assume a investigação

Sem instalação. Em duplas, escolham o próximo salto e sustentem a resposta com uma evidência.

DUAS RODADAS: CAMINHO DO PACOTE E MUDANÇA NO CACHE

EQUIPE 1

BLUE TEAM

Qual configuração ou associação precisa de correção?

EQUIPE 2

RED TEAM

O destino cabe no escopo autorizado e qual caminho ele exige?

EQUIPE 3

FORENSE DIGITAL

O que o registro mostra e que evidência ainda falta?

COMO PARTICIPAR

- Rodada 1: todos votam em entrega local, gateway ou endereço especial.
- Rodada 2: cada dupla formula uma hipótese e pede uma evidência.

Qual caminho a estação A escolhe?

A = 10.10.10.70/26, gateway .65. Caches vazios e nenhuma rota extra, salvo na linha 4.

DESTINO OU SITUAÇÃO	CONTEXTO	DECISÃO DA TURMA
B: 10.10.10.90	Mesma VLAN de A	Local ou gateway? ARP por quem?
C: 10.10.10.130	Outra VLAN	Local ou gateway? ARP por quem?
Portal: 10.10.30.20	Rede remota	Qual IP e qual MAC no quadro?
C: 10.10.10.130	A voltou ao /24	O que muda na consulta ARP?
10.10.10.127	Broadcast do /26	Pode ser IP de um host comum?
Vizinho IPv6 no enlace	Cache IPv6 vazio	ARP ou Neighbor Discovery?

Cada dupla vota e justifica. Para o Red Team, o único bloco autorizado é 10.10.10.64/26.

O MAC do gateway mudou. E agora?

Registros fictícios coletados na estação A, na VLAN 110, depois da correção do /26.

09:20	CONFIGURAÇÃO	A = 10.10.10.70/26. Rota padrão via 10.10.10.65.
09:21	CACHE ARP	10.10.10.65 associado a 02:00:00:00:10:65. Valor esperado.
09:22	ARP REPLY	Mensagem anuncia .65 em 02:00:00:00:ee:01 sem pedido observado.
09:23	NOVO CACHE	A passa a associar .65 ao MAC 02:00:00:00:ee:01.

HIPÓTESE E EVIDÊNCIA

Foi ataque? Que outra explicação existe? Que dados precisamos preservar?

Duas pistas, duas conclusões diferentes

Os endereços explicam o caminho. A conclusão depende da evidência disponível.

01	**Máscara antiga**	A usava /24. A correção para /26 restabeleceu o caminho até C.
02	**Próximo salto**	B é local. C e o portal exigem o gateway, nas rotas deste cenário.
03	**ARP divergente**	O cache mudou. Investigar ataque, failover ou alteração legítima do gateway.
04	**Limite da atribuição**	IP e MAC precisam de horário, interface e correlação com outros registros.

Relato final: falha de configuração confirmada no caso e associação ARP suspeita ainda em investigação.

Três perguntas para fechar a investigação

Responda antes de sair: endereço, próximo salto e evidência.

SUB-REDE

Onde termina?

Qual é a rede e o broadcast de 10.10.10.70/26?

ENTREGA

Qual MAC?

Ao enviar para 10.10.10.130, A procura o MAC de C ou do gateway?

IPv6

Qual descoberta?

Que protocolo procura vizinhos IPv6 e por que a defesa precisa observá-lo?

No próximo laboratório, esse caminho poderá virar uma simulação com pacotes e tabelas visíveis.