SR. ANTÔNIO MARCOS MOREIRAS: Bom dia a todos! Estamos começando mais um dia aqui na Semana de Capacitação On-line do NIC.br.

Hoje temos a participação do Nicolás Antoniello e do Daniel Fink, da Icann. E para quem não sabe o que é a Icann, Icann não é uma empresa, é uma organização. É uma organização que atua na governança da internet, na governança justamente do DNS. Eles são, então, o pessoal da Icann é especialista em DNS, e eles vieram aqui falar para a gente justamente do DNS, mais especificamente como a gente faz um DNS recursivo de forma adequada. Vão falar de Hyperlocal, vão falar de DNSSEC, vão falar de outras coisas aí.

Então, hoje, o tutorial, esse minicurso, ele tem uma parte prática. Quem acompanhou já os outros dias da semana, já estava sabendo, se alguém chegou agora. No site da Semana de Capacitação, semanacap.bcp.nic.br, tem os materiais lá disponíveis para você... as instruções para você instalar uma máquina virtual e acompanhar a parte prática, né? Passo a passo, todos os comandos. Está ali tudo bonitinho. Se você quiser ainda olhar lá esses materiais, baixar e tentar acompanhar a parte prática fazendo junto, você pode fazer isso. Mas mesmo que você não for acompanhar agora, fazendo junto, quem não se preparou antes, né? Talvez fique apertado o tempo para baixar a máquina virtual, para fazer tudo. Mas você ainda assim entra lá no site da Semana de Capacitação e baixa o material. Porque pode ser que no vídeo, por exemplo, aqui no Youtube, os comandos apareçam pequenininhos demais, não dê para acompanhar muito bem, e está tudo lá passo a passo nesse material. Então vai facilitar quando a explicação chegar nessa parte prática que você acompanhe. Daí você fica vendo o vídeo e olhando o material também. E vai tudo funcionar melhor. Então recomendo fortemente que vocês entrem lá no site da Semana de Capacitação e baixem esse material.

Outra coisa, a gente sempre pede, né, eu sempre peço, pelo menos. Deem like no vídeo, né? Vocês que estão acompanhando, vocês que já acompanharam a gente ontem, anteontem, vocês já viram a qualidade do material desses cursos, dessa Semana de Capacitação On-line, vocês podem dar um crédito de confiança na gente e dar o like desde já, mesmo antes da gente apresentar todo o conteúdo técnico, por quê? Porque assim o Youtube, ele distribui o vídeo para mais gente. Não é todo mundo que está inscrito no canal do Youtube que recebe o aviso, a notificação de que a live está rolando, de que o vídeo está acontecendo agora. Agora, quanto mais like, para mais gente o Youtube distribui. Então por isso que a gente insiste, por isso que todo mundo que é youtuber, todo canal do Youtube acaba pedindo esses likes, né? E a gente não vai ser diferente nisso. Se vocês puderem dar like vai ajudar bastante para a gente, vai ajudar bastante a gente a levar esse conteúdo para mais gente. É um conteúdo muito interessante, que pode ajudar muitos provedores. Porque um DNS bem configurado, ele traz, vamos dizer assim, uma maior qualidade, uma maior percepção de qualidade pelos usuários, uma maior velocidade até. É algo que, às vezes, o pessoal simplesmente põe lá um 'ticzinho' de ativar DNS lá no Mikrotik, acha que está tudo bem e não é só isso, né? Tem muita coisa para se fazer pra ficar legal. E nesse vídeo aqui, nesse curso aqui, o Daniel e o Nicolás vão ensinar algumas dessas coisas.

Um outro ponto aí importante é o seguinte: o tutorial que vai ser dado nesse vídeo hoje, o pessoal vai reforçar durante o próprio tutorial, durante a aula, mas eu já digo desde já, não é uma receitinha de bolo pronta para você colocar exatamente igual em produção no seu provedor. Porque tem alguns pontos que são enfocados, que são reforçados nesse tutorial e tem outras configurações necessárias para um servidor de produção que não vai dar tempo de apresentar. O pessoal escolheu reforçar alguns pontos importantes aí, que eu vou deixar para eles falarem aí durante a apresentação do conteúdo. Então façam isso.

O pessoal brinca, muitas vezes, nos vídeos de Youtube: "Ó, não façam isso em casa! Não façam isso em casa!". Então a orientação aqui que o Daniel e Nicolás me passaram antes da gente começar a live é que: "Façam isso em casa!" Não é para colocar em produção exatamente essa configuração. Depois você pode juntar essa configuração com outras boas práticas, aí sim vai ficar uma configuração superlegal para colocar em produção.

Da mesma forma dos outros dias, da Semana de Capacitação, o Daniel e o Nicolás, eles gravaram uma parte do tutorial em vídeo. Por quê? Porque todo mundo está fazendo home office, porque a internet pode cair, e tudo mais. Então a gente vai simplesmente agora dar play numa parte que já está gravada. Mas o Daniel e o Nicolás estão aqui com a gente, estão aqui ao vivo aqui, nos bastidores, e eles estão acompanhando o chat do Youtube. Eu até recomendo, quem estiver assistindo pelo vídeo que está lá incorporado em [ininteligível] no site da Semana de Capacitação, vai direto para a página do Youtube. Pode ir para o Facebook também, tem transmissão no Facebook. Porque daí vocês podem interagir pelo chat do Youtube, ou pelo chat, pelos comentários ali no Facebook. E a nossa equipe, o próprio Daniel e o próprio Nicolás estão acompanhando e vão conseguir responder as dúvidas de vocês ali na hora, pelo próprio chat. E as dúvidas mais importantes, mais interessantes, eles vão entrar depois ao vivo, aqui no vídeo, para responder em viva-voz. Tá bom?

Como nos outros dias da semana, eu vou pedir para o Pedro agora, da nossa equipe técnica aqui, colocar um videozinho de 15 segundos, que é de um projeto novo em que a gente está trabalhando de vídeos educativos para a comunidade de usuários de internet em geral. Então mais para frente, muito em breve, a gente espera conseguir lançar esse projeto, e vocês vão saber mais deles, e eu estou mostrando um videozinho aqui por semana como uma espécie de teasing aí, e até para já pegar alguns comentários de vocês para vocês dizerem se gostaram ou não gostaram desse tipo de vídeo, da forma como eles estão sendo feitos.

Então, Pedro, por favor, dá play no vídeo, depois eu ainda volto aqui pra dar alguns recados que faltaram.

[exibição de vídeo]

SR. ANTÔNIO MARCOS MOREIRAS: Muito bem. Então são alguns vídeos que têm dicas mais técnicas, como o que eu mostrei ontem, anteontem, que era sobre senhas; tem outros vídeos que são dicas um pouco mais comportamentais para os usuários. Tem vários tipos de vídeos que a gente está fazendo aí, ensinando as pessoas a usarem a internet de uma forma mais legal.

Bom, o Nicolás, um dos instrutores aí do curso de hoje, ele não é brasileiro. Ele é uruguaio. Ele também não é argentino não, viu?! Então vocês podem assistir o vídeo tranquilamente, não precisa agora fechar o Youtube, nem nada disso, porque ele não é argentino, tá? Mas ele fala 'portunhol'. Ele fala 'portunhol', mas é mais ou menos, assim, quando eu tento hablar em portunhol: Yo voy pensar hablar en 'portunhol', e para por aqui. Certo? Todo resto sai em português. Então o Nicolás vai falar... o 'portunhol' dele tem bastante sotaque de espanhol, mas, para ajudar vocês, a gente já colocou as legendas todas bem traduzidas e revisadas em português. Então, se alguém tiver alguma dificuldade de entender o Nicolás... Eu acho que vocês não vão ter dificuldade nenhuma. Eu brinquei um pouquinho aqui, mas o 'portunhol' dele é bastante claro. Mas, caso alguém tenha alguma dificuldade, olhe as legendas. As legendas estão traduzidas e revisadas em português. E daí vai ajudar vocês a compreenderem alguma coisa que, porventura, não tenha ficado tão clara na fala, ou por causa do sotaque. Tá bom?

Como hoje, amanhã também tem uma parte prática no tutorial, então quem for acompanhar amanhã também entre lá no semanacap.bcp.nic.br. Veja lá as instruções, baixe lá os materiais que já estão lá disponíveis, prepare aí durante a tarde, hoje à noite as máquinas virtuais para acompanhar a aula de amanhã.

Esse vídeo aqui vai ficar gravado, o Youtube grava. Logo após a live, ele já vai estar disponível de imediato. Então, vocês podem, se quiserem, por exemplo, acompanhar hoje a parte prática só assistindo, e depois prepara o ambiente virtual para testes, e tudo mais, com calma, e assiste de novo, né? Pode... se tiver alguma dificuldade de entender a parte do Nicolás, que está em... naquele 'portunhol', põe para tocar mais devagar, vai parando, vai olhando a legenda. A gente está fazendo de uma forma que vai ficar bem tranquila para vocês acompanharem, para vocês pegarem esse conteúdo, essas dicas do Daniel e do Nicolás, porque elas são importantíssimas para o provedor. Tá bom?

E é isso, gente. Eu vou passar a palavra agora justamente para o Daniel e para o Nicolás para eles darem prosseguimento ao conteúdo técnico. Bom curso para todos.

SR. EDUARDO BARASAL MORALES: Moreiras, você acabou esquecendo de falar do certificado. O pessoal já está escrevendo no chat. Pode falar.

SR. ANTÔNIO MARCOS MOREIRAS: Ah, muito importante, Eduardo. Muito obrigado por me lembrar. Como nos outros dias da live, nós vamos fornecer um certificado on-line, um certificado de participação. Esse certificado é para quem está assistindo aqui ao vivo. E o que vocês têm que fazer? O pessoal vai colocar o link lá no chat, vocês têm que entrar e se inscrever. Como se fosse a inscrição para um curso. Quem não quiser o certificado, não precisa, só assiste aqui, aprende o que tem que aprender e tudo bem. Quem estiver acompanhando aqui ao vivo e precisar do certificado, entra no chat do Youtube, olha lá o link e se inscreve. Tem que fazer isso até as 14h. Quem estiver acompanhando, às vezes, pelo celular: "Ah, não consigo entrar no chat, porque eu estou no celular". Bom, até as 14h entra no computador, pega o link que vai estar lá no chat, se inscreve. E, depois disso, a gente não tem mais como dar o certificado. Certificado é para quem está acompanhando aqui on-line. Então façam um esforço aí e façam essa inscrição até as 14h. Ok? Bom curso para todos.

SR. DANIEL FINK: Alô, pessoal! Muito obrigado aí pela introdução. Bom dia a todos.

Então, o meu nome é Daniel, eu estou aqui acompanhado pelo Nicolás Antoniello que está conectado do Uruguai.

SR. NICOLÁS ANTONIELLO: Bom dia. Bom dia a todos.

SR. DANIEL FINK: Tudo bem? Muito frio por aí?

SR. NICOLÁS ANTONIELLO: Muito frio. Muito, muito frio. Hoje está zero graus.

SR. DANIEL FINK: Está gelado mesmo.

SR. NICOLÁS ANTONIELLO: Sim.

SR. DANIEL FINK: Então tá bom, pessoal. A gente, primeiro, quer agradecer ao NIC.br, a toda equipe por essa oportunidade de trazer esse laboratório pra vocês.

Esse é um material que a gente desenvolveu desde o final do ano passado, para fazer esses cursos presenciais. É o que a gente gostaria, de estar junto com vocês agora, mas ainda bem que a gente pode

fazer essa tentativa de curso online. Vamos adiantar um pouco o assunto e, em breve, se Deus quiser, a gente vai estar reunidos em alguma sala de aula para fazer as práticas da melhor maneira possível. Não é isso, Nico?

SR. NICOLÁS ANTONIELLO: Isso.

SR. DANIEL FINK: Então tá bom, pessoal. Eu vou compartilhar aqui a minha tela, para a gente fazer uma pequena introdução sobre o curso.

Então, hoje, a gente está aqui para falar sobre implementação de servidores recursivos usando o exemplo aí para o BIND e para o Unbound, e verificar o funcionamento do DNSSEC, as extensões de segurança do DNS, e o Hyperlocal.

Bom, vocês devem ter recebido um documento anterior, que a gente explica como configurar as máquinas virtuais que a gente vai usar aqui nesse laboratório. E a gente vai compartilhar com vocês também esse guia da prática que a gente vai apresentar, passo a passo, para depois vocês fazerem em casa e no laboratório de vocês, ok?

Então, vamos lá. A primeira mensagem muito importante que a gente quer trazer para vocês agora é sobre qual é o objetivo desse nosso treinamento. Em primeiro lugar, enfatizar aqui, o que a gente está fazendo aqui é uma prática experimental, uma prática de educação que não serve de maneira nenhuma para ser implementada em um ambiente de produção no provedor de internet de vocês, tá bom? Ainda não. Por que isso? A gente vai explicar como é que o DNSSEC funciona, como é que o Hyperlocal funciona, e a gente vai desconsiderar várias outras coisas que são fundamentais para o bom funcionamento de um servidor de DNS recursivo no provedor, principalmente em relação à segurança. Então, a gente não vai dar muita atenção para a configuração de firewalls, inclusive, no caso do Unbound, a gente vai trabalhar com ele desligado, a gente não vai dar muita atenção para abertura, fechamento de portas, a gente não vai falar de redundância de servidores. Ou seja, vários aspectos que a gente precisa de mais sessões para explicar pra vocês, tá? Mas o que a gente quer mostrar aqui, principalmente para quem já tem algum servidor de DNS recursivo instalado, como poderiam habilitar o DNSSEC com alguma facilidade. E olhando um pouco mais para o futuro, como é que poderiam implementar o Hyperlocal também, que a gente vai explicar com detalhes como é que ele funciona, tá bom? Então, façam isso em casa, façam isso no laboratório, mas não façam no provedor, ok? Essa não é uma recomendação de operação, mas sim uma simples aula, onde a gente vai demonstrar esses conceitos, tá bom?

Sempre abertos para sugestões, mandem suas críticas. A ideia aqui é fazer amigos, e a gente está à disposição para ajudar vocês nos testes que vocês desejarem, tá bom? Está aqui o meu e-mail, está aí o e-mail do Nicolás também. É isso, Nico? Esqueci alguma coisa?

SR. NICOLÁS ANTONIELLO: Sim, um comentário. É que, como você dizia, Daniel, se você já tem um servidor recursivo operando, em operação, este exemplo de configuração que nós vamos mostrar hoje, pode servir para você, para configurar, para agregar ao seu servidor recursivo DNSSEC ou agregar ao Hyperlocal, ou agregar aos dois. Mas se você não tem servidor recursivo operando, provavelmente essa não é a melhor maneira de configurar, principalmente porque você tem que levar em consideração outras questões de segurança, principalmente questões de segurança que não são parte desse tutorial. Então, é muito perigoso, se você não tem um servidor operando, pegar esse exemplo e colocá-lo em produção. E outra coisa mais, as versões que nós utilizamos, de servidores, por exemplo a versão do BIND, depende da versão que você escolher para baixar e colocar em produção. Existem diferentes versões, dependendo se

você quer melhor estabilidade, se você quer melhor segurança, se você quer ter os últimas features. Então, existem questões que não estão, não estão... nós não vamos falar disso nessa apresentação.

Então, tenham em mente realmente isso, que isso não foi pensado para que você comece do zero, com um servidor recursivo em produção. É preciso que você adquira experiência, aprenda e pratique, e brinque com isso, e aí siga avançando até chegar em algo que possa colocar, de forma segura, em produção.

SR. DANIEL FINK: Legal, perfeito. Então tá bom.

Pessoal, passando aqui para a primeira parte, trazendo alguns conceitos que a gente vai utilizar aqui. A gente trouxe algumas figuras que eu acho que são bastante didáticas para exemplificar o que a gente vai implementar. Primeiro, sobre o conceito de DNSSEC. Eu gosto muito dessa figura porque ela representa os componentes que o DNSSEC agregou ao DNS tradicional, para fazer a autenticação das requisições, certo? Então aqui, na parte de cima, a gente tem o servidor autoritativo, que possui as respostas para as consultas do servidor recursivo. O que o DNSSEC tenta fazer é trazer uma forma de verificação, se a informação não foi alterada no meio do caminho, entre a comunicação do servidor autoritativo com o servidor recursivo. Tudo bem? Então, aqui a gente vê que o servidor autoritativo, quando recebe uma consulta de DNS e vai enviar a resposta para o servidor que solicitou, o recursivo, ele vai agregar à resposta uma assinatura digital, certo? Está aqui no quadradinho azul, que é composta por uma Hash do conteúdo que ele está transmitindo, que é uma codificação do conteúdo que ele está transmitindo, assinada por uma chave privada que o DNSSEC utiliza, e que essa chave privada só fica armazenada de maneira segura dentro do servidor autoritativo, tá bom? E aí transmite, então, a informação junto com a assinatura. E quando o servidor recursivo recebe essa informação, ele recebe a resposta que o servidor autoritativo mandou, de maneira aberta, texto puro, e recebe também o código da assinatura digital, tá?

Nesse ponto, na parte mais embaixo aqui da figura, a gente vê que o servidor recursivo faz duas coisas: ele também cria uma Hash igual a que o servidor autoritativo fez; e ele também pega a assinatura digital que foi enviada pelo autoritativo e, combinado com a chave pública da zona, do domínio que ele está sendo recebido, também gera uma nova Hash para poder comparar. Então, se a informação que ele recebeu tem uma Hash, e a informação da assinatura que ele recebeu também vai sair outra Hash, na comparação, se elas forem iguais, a informação está autenticada, o servidor recursivo consegue verificar que a informação não foi alterada durante o percurso da informação pela rede, ok?

Então, é mais ou menos isso, de uma maneira bem resumida que o DNSSEC faz. É claro que ele tem várias elegâncias na sua implementação, que, para quem quiser, estão aqui referenciadas as RFCs que explicam isso com detalhes.

Aqui também, o link para o artigo do Wiki do Brasil Peering Forum, que explica mais detalhes sobre DNSSEC para quem quiser consultar. Legal?

E trazendo aqui também um pouco de fundamentos a respeito do Hyperlocal. O Hyperlocal é uma técnica, que foi recentemente padronizada através de uma RFC, atualmente é a RFC8806, ela é uma nova versão de uma RFC anterior, que também tratava do mesmo assunto, que era a RFC7706. E o Hyperlocal é uma técnica bastante interessante, que consegue colocar uma cópia da zona dos servidores-raiz dentro do nosso recursivo, ok? Então, essa técnica consegue trazer para a gente alguns ganhos de desempenho, como a gente vai ver agora durante a implementação, e também adiciona uma boa resiliência, uma boa robustez ao DNS como um todo. Dado que, caso ocorra alguma indisponibilidade entre os servidores-raiz,

servidores recursivos com Hyperlocal implementado, não deixam de funcionar, não deixam de resolver as consultas, tá bom?

Aqui é uma figurinha de uma resolução de DNS normal, vocês conhecem. Passo um, dois, três. Pergunta para os autoritativos até encontrar o número IP do site que a gente quer resolver. Lembrando que o passo 1 sempre é a consulta para o servidor-raiz, certo?

Quando a gente vê aqui o... como é que o Hyperlocal funciona - essa é uma maneira que eu encontrei para representar -, o Hyperlocal coloca um atalho dentro do servidor recursivo e ele não precisa mais ir para a rede, ir para a internet encontrar um servidor-raiz e fazer a primeira requisição na cadeia de consultas de resolução de um determinado nome. Por que ele pode tomar esse atalho? Porque ele já vai ter um arquivinho, chamado root.zone, armazenado dentro do recursivo, e ele vai poder consultar diretamente. Esse arquivo, normalmente, é pequeno, a gente vai ver durante a prática, não pesa muito no servidor recursivo, e essa implementação traz alguns ganhos interessantes para a gente. Legal? É isso, Nico? Esqueci de alguma coisa?

SR. NICOLÁS ANTONIELLO: Não, tudo bem.

SR. DANIEL FINK: Então, tá bom. Agora a gente vai passar pra primeira parte da prática, eu vou explicar sobre Unbound no CentOS. E, no final, o Nicolás vai explicar sobre o BIND no XUbuntu. Legal? E a gente se vê no final das apresentações, no final das práticas, para a parte de perguntas e respostas.

Valeu, até mais!

SR. DANIEL FINK: Bom, pessoal, vamos passar para a parte da configuração do nosso Unbound, no CentOS8. A gente já está aqui na tela com o documento aberto de um lado, do outro lado nosso VirtualBox. Está aqui a nossa máquina virtual CentOS8-Lab, novinha, sem nenhuma configuração, e aqui no documento a gente vai seguir o passo a passo, e lembrando que o Unbound é uma das opções de servidor de DNS recursivo, é um software de bastante reputação. Se precisar de mais detalhes sobre o Unbound, quem quiser saber mais, está aqui o site pra visitar.

Então vamos lá. Aqui no nosso VirtualBox, primeira coisa que a gente vai fazer é abrir a página de configurações, lembrando que aqui na tab Rede é importante manter a conexão da placa em modo Bridge. É só deixar essa opção aqui marcada, quem não tiver, pode marcar. Isso vai fazer com que a nossa máquina virtual receba um IP automaticamente da nossa rede aqui do laboratório, ok? A gente vai dar um ok aqui, e o próximo passo então seria clicar aqui no botão Iniciar. Agora, a máquina já está inicializando. Enquanto isso, a gente aproveita para andar com o nosso manual... Que a gente já tem o terminal da máquina, com ela fazendo a sua primeiríssima inicialização. Vamos aguardar um pouquinho, meu PC aqui não é dos mais rápidos do mundo. Pronto, já estamos aqui com a primeira tela de login, e a gente vai logar com o usuário root e a senha aqui, conforme nosso manual, icannlab2. Beleza. Primeira coisa que a gente vai fazer, pessoal, é ver qual é o IP que a nossa máquina recebeu. Pra isso, a gente vai usar o comando ip addr, bem simples, e vamos lá. Vou tomar nota aqui na minha colinha, o IP que a nossa máquina recebeu está apontado aqui: 192.168.0.117, na rede /24. Muito bem. Difere um pouco aqui do nosso manual, mas não tem problema, basta a gente anotar e lembrar ele daqui a pouquinho.

Vamos passar agora pra parte de preparação do servidor? Vou usar esse mesmo terminal aqui do VirtualBox, depois a gente aumenta o tamanho da letra, usa um terminal um pouquinho melhor, que é o PuTTY, mas vou aproveitar aqui, já vou fazer a primeira instalação dos pacotes necessários pra gente fazer a instalação do Unbound. Vou usar o comando aqui yum install e eu vou trazer aqui pra nossa máquina o

editor de texto nano, net-tools, vou trazer o wget, vamos trazer o, claro, o Unbound e vamos trazer o bind-utils. Cada um desses pacotes possui ferramentas que a gente vai utilizar aqui na prática. No manual aqui a gente está com esse comando em duas linhas, não tem problema fazer uma linha de cada vez. Eu só coloquei todos juntos aqui pra facilitar, essa linha toda junta ia quebrar a referência pra vocês aqui, no documento. Vamos lá. Está baixando os pacotes. A gente precisa dar algumas configurações, aguardar um pouquinho pra chegar tudo. E concluído. Interessante ver aqui que a versão do Unbound que a distribuição do CentOS traz pra gente é a 1.7. Interessante lembrar isso quando a gente for fazer configurações. Legal.

Vou dar uma limpada aqui na tela, e agora, pessoal, é uma parte que a gente vai usar exclusivamente aqui no nosso laboratório, pra fins de aprendizagem. A ideia não é utilizar esse tipo de configuração para produção, não é para utilizar para os clientes de vocês, mas sim pra gente simplesmente fazer uma demonstração do funcionamento do DNSSEC e do Hyperlocal aqui nesse caso. Então, nós vamos desabilitar o Firewalld e o SELinux pra agilizar aqui a nossa prática, mas lembrando que isso são requisitos obrigatórios pra gente ter um servidor de produção, mas não é o tema exato desse nosso curso. Então, procurem auxílio, procurem ajuda quando forem configurar uma máquina dessas em produção. Pra quem já tem, vale o que a gente disser aqui pra complementar a configuração de vocês, mas caso vocês desejem realizar essa prática aqui na casa de vocês, no ambiente de vocês, não coloquem esse tipo de configuração nos sistemas de produção que vocês possuem. Então, a gente já comentou sobre isso, mas não custa eu lembrar.

Então, vou primeiro desabilitar aqui o Firewalld, pronto, e pra desabilitar o SELinux a gente vai usar o Nano pra acessar o arquivo de configuração do SELinux, que está no /etc/selinux/config. A gente entra no arquivo de configuração do SELinux, que é aqui na parte do enforcing, a gente vai colocar aqui exclusivamente para o nosso laboratório o comando disabled. Ctrl+X pra sair do Nano, yes pra salvar o arquivo e pronto. Bom, feito isso, a gente precisa reinicializar a nossa máquina. Vamos dar aqui um init 0 e daqui a pouco a gente volta com o próximo login.

Legal, a máquina já desligou, o que a gente vai fazer agora é iniciar ela novamente... Pronto, já temos aqui a nossa pasta inicializada, vamos logar novamente. Usuário root, senha icannlab2, legal. Podemos verificar aqui se o Firewalld está realmente desabilitado. Legal, pronto. Agora a gente já está praticamente pronto pra começar a preparação do Unbound, mas eu vou aproveitar agora pra abrir um terminal com letras um pouco maiores, pra facilitar a visualização de vocês, através do PuTTY. Tá legal, a gente já está aqui com a telinha do PuTTY pra fazer a conexão na nossa tela, que a gente vai fazer aqui no PuTTY, que é um terminal de acesso SSH, nós vamos colocar o IP da nossa máquina, que foi o 117, clicamos aqui no Open, e legal, já temos um terminalzinho aqui do PuTTY. O bacana do PuTTY é que a gente pode facilmente copiar do nosso documento e colar aqui no terminal. Eu vou aumentar aqui um pouco o tamanho da letra. Vamos lá, aparência... Vou usar aqui uma fontezinha Terminal mesmo, tamanho 14, apply, beleza. Vamos logar aqui novamente com o PuTTY, e pronto, já estamos acessando a nossa máquina virtual, através do PuTTY. Vamos lá.

Preparando o Unbound, vamos acessar então a nossa pasta /etc/unbound, que acabou de ser instalada. Vamos dar uma olhadinha nos arquivos dessa pasta, através do ls -l. Bacana. Temos aqui seis arquivos instalados, originalmente. A gente vai fazer agora, pessoal, a remoção de dois arquivos, o unbound.conf e o root.key, pra gente criar eles novamente com as configurações aqui da nossa prática, tá? Antes disso, vamos dar uma olhadinha no unbound.conf, qual é o arquivo de configuração original que vem nele. Vocês podem ver que é um arquivo bastante complexo, tem todos os comandos aqui descritos, é praticamente um tutorial de configuração do Unbound, ele tem vários recursos e aqui pra nossa prática a gente vai criar

um outro bem simplificado, simplesmente pra demonstrar o DNSSEC e o Hyperlocal, ok? Vale a pena, pra quem quiser se aprofundar, estudar mais recursos que o Unbound possui, e uma ótima referência é o unbund.conf, ok? Então, a gente vai remover aqui o unbound.conf, através do comando rm. Vou trazer aqui pro terminal. Olha, removi o unbound.conf e eu vou remover aqui o arquivo root.key também, que já vem configurado nele, mas a gente vai demonstrar um comando que faz justamente a criação desse root.key. E pra que serve o root.key então? O root.key, ele possui a chave pública do DNSSEC para a zona-raiz do DNSSEC. Então, ele vai ser utilizado pra auxiliar na autenticação das validações do DNS. Muito importante ter ela atualizada e configurada no servidor. Então, agora a gente deleta, para criar ela depois, bacana?

Então, fizemos essa primeira parte, e agora a gente vai passar pra trazer um recurso pro nosso Unbound, que é o arquivo named.root. O arquivo named.root está disponível no site internic.net. esse arquivo contém a primeira referência que o servidor recursivo vai utilizar nas suas consultas, que é a lista dos servidores-raiz do DNS. Então, o wget vai trazer aqui pra nós, um download rápido, e pronto, creio que ele já está aqui. Vamos dar uma olhada: ls -l, bacana, está aqui o named.root. Vamos aproveitar aqui, seguindo nosso cronograma, fazer uma breve pausa pra espiar dentro do named.root, o que está escrito ali dentro. Então vamos lá: named.root, qual é a primeira cola que o nosso Unbound vai utilizar pra fazer iniciar as consultas recursivas? Então está aqui, o named.root possui uma lista dos servidores-raiz, organizados aqui, de acordo com cada rótulo, desde o servidor-raiz A até o servidor-raiz M. São os 13 rótulos de servidor-raiz disponíveis no DNS. Traz aqui também, além do nome do servidor, os números de conexão pra IPv4 e IPv6.

Muito bem. Ctrl+X agora pra sair do Nano, não precisa salvar, vamos dar um clear aqui na nossa tela, e passando pra próxima parte sobre então a edição do nosso novo arquivo de configuração do Unbound. Vamos criar agora um arquivo unbound.conf, podemos usar o mesmo comando nano unbound.conf. Arquivo em branco, arquivo novo. Eu vou trazer aqui, pessoal, a nossa primeira sugestão de configuração simplificada do Unbound pro arquivo unbound.conf. A gente trouxe aqui o texto, a configuração do Unbound sempre começa com server:, depois aqui a gente vai especificar onde ele está sendo executado, na pasta /etc/unbound, onde estão os arquivos do Unbound. Interface 0.0.0, a gente vai deixar aqui pra ele ser controlado por qualquer interface. E aqui, a parte de controles de acesso, access control, deixamos aqui três linhas. A primeira delas, ele vai recusar todas as requisições que não vierem das faixas de IP que a gente está especificando aqui nas duas linhas seguintes, então o que não vier das faixas 192.168.0.0/24, ele vai atender, está aqui comando allow pra permitir isso. Consultas locais também, a gente está configurando ele pra responder, através do 127.0.0.0, e o que for fora disso, ele não vai responder, ele não vai resolver para os usuários que não estiverem dentro dessas faixas de IP. Muito importante configurar isso em todo o provedor, caso contrário a gente tem um distribuidor recursivo aberto, e isso é muito perigoso, desnecessário fazer, tá?

Seguindo aqui, porta 53, a porta de comunicação do DNS, e aqui abaixo a gente está dizendo pra ele pra utilizar UDP, sim, utilizar TCP, sim, vai utilizar IPv4, sim, e utilizar IPv6, a gente poderia dizer que sim, mas aqui no nosso caso... A gente deveria dizer que sim, claro, mas aqui no nosso caso a gente não está com o IPv6 configurado na nossa rede de laboratório, então a gente vai deixar por enquanto no, tá legal? Então tá bom. Temos aqui a nossa primeira configuração do Unbound, ultrassimplificada, só pra verificar o funcionamento. E pra sair aqui do Nano a gente vai dar um Ctrl+X, dizer que sim, pode salvar, e escrevemos então o arquivo unbound.conf. Vamos verificar aqui se ele foi criado. Legal, está aqui, no último ponto, unbound.conf, criado pelo usuário root, tá? Bacana. Seguindo aqui o nosso programa, a gente pode utilizar o comando unbound-checkconf, que é um recurso do próprio Unbound, que verifica se

o nosso arquivo de configuração possui algum erro, que ele consiga detectar. Aqui no caso, a resposta foi que não, está tudo bem com o nosso primeiro arquivo.

E agora, pessoal, vamos dar um clear aqui. A gente precisa fazer um ajuste nas permissões. Lembram que a gente especificou que o Unbound vai operar através do usuário unbound, dentro dessa pasta? Então, uma ação importante a fazer é alterar as permissões, aquilo que foi criado pelo nosso usuário-raiz, nosso usuário root. A gente vai organizar aqui direitinho pra ele, para as permissões todas ficarem embaixo do usuário unbound. Pra isso, a gente vai usar o comando chown, configurado aqui pra transferir todos os arquivos de maneira recursiva para o usuário unbound. Legal? A gente vai repetir esse comando algumas vezes, mas, por enquanto, está tudo bem. Agora, estão todos aqui abaixo, com permissão para o usuário unbound.

Legal. Chegou a hora então da gente habilitar o serviço do Unbound no nosso CentOS e iniciar o serviço também. Vamos lá: systemctl enabled unbound. Bacana, habilitamos o serviço. A seguinte, vamos iniciar o serviço do Unbound então, systemctl start unbound. Legal, serviço iniciado. E, por fim, podemos verificar aqui qual é o status do Unbound depois da nossa ativação: systemctl status unbound. Legal, ativo, rodando, bacana. Podemos partir agora para o nosso primeiro teste. Vou limpar aqui a tela, e pra isso eu vou utilizar o comando dig pra fazer a primeira resolução do nosso Unbound, dig apontando pra nossa própria máquina, 192.168.0.117. Esse é o servidor que eu quero consultar, que acabamos de configurar e vamos resolver aqui o nome do site, nic.br. Legal, temos aqui a nossa primeira resolução do Unbound, para o site nic.br. Tempo de resposta, 258 milissegundos. Bacana. Temos o Unbound funcionando, parabéns.

Pessoal, agora, pra facilitar os nossos próximos testes, eu vou mudar o arquivo resolv.conf, que está configurado com o DNS que foi informado pelo DHCP na inicialização dessa máquina. Vamos dar uma olhada aqui no resolv.conf, está no /etc. Podem ver aqui que ele está apontando o nameserver pro nosso roteador, vai mudar aqui pra ele apontar todas as consultas de DNS, por padrão, nessa máquina, para a porta local: 127.0.0.1, ok? Vou dar um Ctrl+X aqui pra sair, salvar o arquivo... Bacana. Então agora se a gente fizer o mesmo comando, dig.nic.br, a gente já tem automaticamente a resolução sendo direcionada pra nossa porta local, é o nosso Unbound que está respondendo. Bacana, isso vai ajudar bastante daqui pra frente.

Legal, continuando aqui, vamos falar um pouquinho sobre esse comando que eu acabei de utilizar, o dig. Ele é o Domain Information Groper, ele consulta informações no DNS pro nosso terminal, muito útil pro nosso treinamento, muito útil pra troubleshooting aí no dia a dia do provedor, e ele é um componente do pacote BIND, esse que nós instalamos no início da configuração, tá? A sintaxe dele é o dig, o servidor que a gente quer apontar a consulta, vai na frente ali o arroba, em seguida a gente tem o recurso que nós queremos consultar, o nome do site que nós queremos consultar, ou o número IP que nós queremos consultar, e o tipo de registro de recurso que nós queremos trazer, tá bom?

Aqui, alguns exercícios pra gente exemplificar o uso do dig. O primeiro exercício que a gente vai fazer é simplesmente digitar o comando dig, sem nenhuma outra informação, e vamos ver o que ele traz. Bom, o dig puro e simples, ele traz pra gente a lista de servidores-raiz do DNS. Aqui, a gente tem a listagem dos servidores-raiz, desde o A até o M, quais são os números IPv4, os números IPv4 e os IPv6, e o query time, como vocês podem ver, é de 0 milissegundos. Isso quer dizer: essa informação está vindo do arquivo named.root, que a gente acabou de baixar, e é a primeira referência, como eu falei nas consultas de DNS dos servidores recursivos, ok?

Bacana. Passamos aqui para o próximo exercício. A gente pode fazer um dig pro seu site favorito, vamos colocar aqui o meu... Vamos fazer uma consulta aqui pro site da Icann, icann.org é o recurso que eu quero consultar, e eu quero saber os registros A do site, do domínio icann.org. Faço a consulta aqui, legal, recebi a resposta do DNS: registro A do site icann.org, 192.0.32.7. Muito bem. Podemos fazer isso também pro registro de recurso de e-mail, que é o registro MX. Vamos tentar aqui pro lacnic.net, quero saber quais são os servidores de correio eletrônico vinculados ao LACNIC. Vamos lá, mando a consulta pelo dig, temos aqui duas respostas: o servidor de correios registro.lacnic.net e o mail.lacnic.net. Muito bem. Essa consulta levou 119 milissegundos pra ser resolvida pelo nosso Unbound. E a gente pode também fazer uma consulta de algum nome que não existe no DNS, digamos assim. Nosso próximo exercício, dig dominioquenaoexiste.tldqnaoexiste. Certamente não está na base de nenhuma zona esse domínio e a gente faz a pergunta pro DNS. O que ele vai nos responder é que a nossa pergunta, opcode: QWERY aqui, teve um status de domínio não existente. Então, está aqui a nossa resposta. A gente pode ver que, na parte de resposta à nossa consulta, o nosso domínio que não existe, aqui, não retornou nenhum número IP vinculado a ele, e é isso que a gente espera, tá?

Passando aqui pra mais um exercício, a gente pode fazer um dig para um outro servidor de DNS, aqui vamos utilizar o DNS público do Google, o 8.8.8. O seu site favorito, vou digitar aqui, por exemplo, o nic.br, e temos a resposta então do servidor do Google, para o nic.br, resolvendo para o IP do próprio nic.br.

Muito bem. A gente trouxe aqui também pra vocês, pessoal, um bônus, uma outra configuração do comando dig, que serve pra fazer uma consulta interessante, ou seja, saber quanto tempo leva pra um servidor-raiz responder pra nossa máquina, onde que ela está localizada, qual é o mais rápido. A gente pode fazer esse exercício através dessa série de comandos. Eu vou trazer aqui pro terminal, a gente vai estar dando um dig, consultando o servidor-raiz L, que está aqui logo depois do arroba, e essas demais configurações aqui vão trazer pra gente qual é o servidor-raiz que recebeu essa consulta e está nos mandando uma resposta, e quanto tempo levou pra ele responder. Então, a gente tem aqui uma instância do servidor L, que provavelmente foi instalada pelo nic.br, está localizada aqui em São Paulo, e aqui no meu caso levamos 4 milissegundos pra receber a resposta dele, tá bom? Dá pra brincar bastante com esse comando, simplesmente trocando aqui de L pra outro rótulo de servidor-raiz. Vamos consultar agora qual é o servidor A, mais próximo, que é o primeiro que responde. Está aqui, ele levou um pouco mais de tempo, 139 milissegundos, e talvez aqui pelo código, eu não tenho certeza, mas eu acho que ele não está no Brasil. Legal, dá pra fazer esse exercício até o M. Fazer um último aqui, vamos consultar aqui pro B, legal, o servidor-raiz B, então, levou 110 milissegundos pra responder, e ele está localizado provavelmente aqui em Miami. Bacana? Então tá bom.

Seguindo aqui, pessoal, vamos fazer mais uma última explicação sobre os recursos que o dig nos traz, vamos trazer aqui uma nova consulta, vamos verificar agora o site example.com, perguntando pra ele quais são os name servers do example.com. Um pouco mais de detalhes aqui sobre o que o dig nos informa. Já falamos aqui que o opcode aqui é o de pergunta padrão, do nosso recursivo para o DNS em geral. Nós tivemos aqui como status da resposta nenhum erro. Ele conseguiu resolver e esse campo aqui das flags, é interessante, a gente vai comentar mais sobre ele na parte de DNSSEC, a gente teve aqui que a flag rd, por exemplo, configura que a recursão foi desejada, ou seja, ele perguntou pra todos os servidores autoritativos apontados pra ele e 'ra' quer dizer que a recursão estava disponível. E nós tivemos aqui duas respostas, duas answers pra servidor de nomes do site example.com, do domínio example.com, que são o a.iana-servers.net e o b.iana-servers.net. Legal. Bacana saber essas possibilidades do dig pros nossos troubleshootings, tá?

Agora a gente vai passar pra parte de implementação do DNSSEC no nosso Unbound. Antes disso, pessoal, vamos fazer mais um dig aqui para um site interessante pro nosso troubleshooting. Vamos fazer um dig pro site dnssec-failed.org. Esse domínio foi criado especificamente pra fazer testes de DNSSEC. Na realidade, o nome dele é failed, porque ele possui registros de recurso de DNSSEC propositalmente errados, ele foi feito pra falhar em caso de autenticação, certo? Então, se esse domínio resolver no nosso servidor recursivo, o DNSSEC não está implementado. Caso ele não resolva e nos retorne erro, quer dizer que o DNSSEC funcionou e está operando a contento. Então, vamos fazer essa consulta aqui de dig ao dnssec-failed, pro nosso Unbound, ainda sem DNSSEC habilitado, e vamos analisar aqui a resposta. Bom, ele mostrou isso aqui no status, não teve problema nenhum pra fazer essa consulta, ele não considerou os registros de recurso do DNSSEC e nos trouxe então que o número IP do dnssec-failed é esse 69.252.80.75. Caso essa resposta tenha vindo de um domínio com seu número IP comprometido, que direcione pra um site de algum atacante ou de algum... ou de alguma operação maliciosa na internet, a gente vai ter a conexão acontecendo e os nossos clientes expostos aí a esse tipo de vulnerabilidade. Então, é isso que o dnssec-failed demonstra. Nesse caso aqui, resolveu com sucesso a requisição, e isso não deveria acontecer.

Legal. Vamos guardar essa informação aqui de como foi a resposta ao teste do dnssec-failed, e partir agora então pra implementação do DNSSEC no nosso Unbound. Vou limpar aqui a nossa tela e, bem, primeira atividade aqui do nosso guia é fazer, é remover o arquivo root.key. Nós já fizemos isso lá no início, ele já está removido aqui dos nossos arquivos, no Unbound, e o que a gente vai fazer agora é utilizar um recurso do Unbound pra fazer a criação do root.key, desse arquivo, que nada mais é do que a chave pública do DNSSEC. Então, utilizando aqui o unbound]#, nós vamos solicitar pro Unbound criar esse novo arquivo, root.key. Sucesso, tivemos a criação, podemos verificar aqui com o ls -l, e aqui está ele, root.key, criado nos nossos arquivos para o Unbound. Muito bem. Novamente, a gente vai trocar a permissão dos arquivos para o usuário unbound, dado que a gente acabou de criar o root.key. Vamos verificar aqui, pronto, está todo mundo devidamente permissionado para o usuário unbound.

Limpando aqui a tela, e vamos voltar agora, pessoal, pras reabilitações do DNSSEC, vamos voltar para o arquivo de configuração do Unbound. Olha, esse é o arquivo que nós criamos há pouco e aqui no nosso guia nós temos o comando que a gente vai colocar no arquivo de configuração, pra iniciar a autenticação das consultas de DNSSEC, que nada mais é do que essa linha de comando aqui. Comentado aqui que essa é a parte do DNSSEC, e esse é o comando auto-trust-anchor-file, então a gente está dizendo pro Unbound que ele pode confiar na chave root.key, que nós acabamos de criar, que é a âncora de confiança, a chave pública de autenticação do DNSSEC para a configuração. A gente está usando aqui o comando, parte do comando é o auto, isso faz com que o próprio Unbound possa verificar se ocorrer alguma atualização nesse arquivo, nessa chave que está armazenada no arquivo root.key. Se ocorrer alguma atualização com essa chave, ele vai atualizar ela automaticamente, ok?

Então, já temos aqui o nosso DNSSEC configurado, é simplesmente isso, uma linha de comando dentro da nossa configuração do Unbound. Saímos aqui do nosso editor de texto, arquivo salvo, podemos fazer uma verificação aqui do nosso arquivo de configuração, unbound-checkconf. Legal, sem erros, e... Movendo aqui o nosso guia.

Próximo passo então para fazer o DNSSEC funcionar é reiniciar o serviço do Unbound: systemctl restart unbound. Legal, Unbound reiniciado, podemos fazer um teste agora, fazer uma nova requisição dig pro site do nic.br, que a gente sabe que está com o DNSSEC muito bem configurado no servidor autoritativo. Vamos perguntar então agora, pedir pra ele fazer a consulta, uma nova consulta, e acrescentar aqui que a gente quer dar uma olhada nos parâmetros de DNSSEC do nic.br. Bom, vamos verificar aqui a nossa

resposta e agora a gente tem algumas novidades. Aqui na parte das flags, a gente tem uma flag diferente, a flag ad, a flag de autenticação. Essa flag sinaliza que a resposta que nós recebemos do servidor autoritativo está autenticada pelo nosso servidor recursivo. Legal, DNSSEC funcionando, autenticou, não houve erro e ele também trouxe pra gente o novo registro de recurso do DNSSEC, que é RRSIG, que é a assinatura digital do domínio nic.br. Legal? Tempo de resposta, 170 milissegundos, e primeiro teste executado com sucesso.

Muito bem, vamos dar um clear aqui na nossa tela e voltar a falar do nosso amigo, dnssec-failed.org. Agora, a gente pode verificar como é que o nosso Unbound se comporta face a um problema de DNSSEC, talvez algum ataque, talvez alguma má configuração. Então, vamos fazer a consulta aqui de novo pro dnssec.org, lembrando que, da última vez, ele resolveu, não conseguiu autenticar, e agora... Ele até levou um pouco mais de tempo pra passar a resposta. A gente vê aqui que não temos a flag de autenticação da resposta, algum problema aconteceu e o status então, falha no servidor, falha na autenticação. Então, aqui a gente vê com bastante clareza que o domínio dnssec-failed.org não foi resolvido. Por quê? Porque nós não temos um registro A, um número IP vinculado a esse domínio, pra fazer a conexão das nossas aplicações, ok? Então aqui é o DNSSEC funcionando como ele tem que funcionar, trazendo essa camada de proteção para os nossos clientes, caso alguma coisa errada aconteça no trânsito entre a resposta dos servidores autoritativos e o nosso servidor recursivo. Legal?

Então tá bom, pessoal. Podemos fazer mais alguns, alguns testes aqui, podemos utilizar o dig pra perguntar para o servidor, digamos, do nic.br, qual é a chave pública do domínio do nic.br, que no caso é o registro de recurso dnskey. Legal, temos aqui a chave pública do domínio do NIC. Podemos verificar também qual é o registro DS, ponteiro pra cadeia de confiança, ele traz aqui pra gente também, na consulta do dig, e podemos perguntar pra ele também, afinal de contas, qual é a assinatura digital que o Unbound está utilizando pra fazer a autenticação, rrsig. Legal, estão aqui as assinaturas digitais pro domínio do nic.br. A gente vê que são alguns recursos adicionais, são novos registros de recursos que o DNSSEC colocou nas zonas de DNS, e são eles que executam esse trabalho de autenticação que a gente precisa. Legal? Bom, concluímos a parte de configuração do DNSSEC.

Aqui, uma pequena explicação sobre como criar uma exceção. Caso vocês desejem criar uma exceção dentro do unbound.conf, vocês podem usar o domain-insecure e o site que vocês querem resolver sem fazer autenticação. Talvez seja um recurso interessante, quando ocorrer alguma requisição especial dentro da rede de vocês.

Ok. Então, concluímos a parte do DNSSEC, vamos passar agora para a parte de configuração de Hyperlocal, no nosso Unbound. A gente trouxe aqui uma curiosidade pra vocês, saber qual é o principal trabalho dos servidores-raiz típica. A gente vê aqui que 65% da carga dos servidores-raiz é dedicada a domínios que não existem, ou seja, digitações erradas, provavelmente, dos usuários, nos seus browsers, e provoca que o servidor-raiz tenha que informar que um determinado domínio não existe, né? Esse tipo de resposta é muito mais frequente do que as respostas de consultas existentes, representadas aqui pela parte verde. Então, mostra que bastante da carga que os nossos servidores recursivos enviam para os servidores-raiz podem ser, digamos assim, atalhadas, através da implementação de uma cópia da zona-raiz, dentro do próprio recursivo, que é exatamente o que o Hyperlocal faz, e a gente vai mostrar aqui como fazer essa configuração no nosso Unbound.

Primeira coisa aqui, antes da implementação, pessoal, a gente vai fazer um teste com o nosso Unbound, que não está ainda com o Hyperlocal implementado. A gente vai dar um dig pra um domínio que não existe. Pode ser um domaininvalid.com.br.xxx, ou dominioqnaoexiste.tldqnaoexiste. Então aqui, a gente

vai forçar o nosso Unbound a fazer a pergunta a algum servidor-raiz. Vamos ver qual é a resposta. Então, a resposta veio que o domínio não existe, chegou do servidor-raiz, não trouxe nenhum IP relacionado a ele, claro, e esse tempo de ida e volta para o servidor-raiz, aqui no meu caso, levou seis milissegundos. Vocês podem fazer esse teste na máquina de vocês também, ok?

Então legal, já temos isso, já em mente, vamos ver o que o Hyperlocal pode fazer por nós e vamos entrar então na nossa boa e velha configuração do unbound.conf e passar aqui pra parte de configuração do Hyperlocal no Unbound. Vou trazer ela aqui pro nosso terminal. Pronto, já copiamos aqui a configuração. Então basicamente essa configuração é apropriada para o Unbound 1.7. As versões mais novas do Unbound, é interessante conferir que a configuração do Hyperlocal está cada vez mais integrada ao software, então as linhas de configuração necessárias são cada vez mais enxutas, mais curtas. Se não me engano, na última versão do Unbound, na 1.9, só são necessárias três linhas de configuração pro Hyperlocal funcionar. É uma tendência interessante. Tem atualizações bastante bacanas de se ler dentro da RFC 8806, que especifica o Hyperlocal.

Então aqui, basicamente, a gente está dizendo pro Unbound que ele pode baixar uma cópia da zona-raiz, através de um desses servidores-raiz, e ele vai armazenar essa cópia dentro do arquivo root.zone, ok? Então, eu simplesmente salvo essa configuração dentro do meu unbound.conf, tá? A gente espera que o Unbound crie automaticamente esse arquivo, root.zone. Só vamos dar uma olhadinha aqui, ver se ele já não existe. A gente vai ver que não, ainda não temos o arquivo root.zone, e pra fazer então o Hyperlocal funcionar, vamos fazer aqui a nossa checagem de configuração. Sem erros, legal. E por fim, a gente só precisa reiniciar nosso Unbound: sistemctl restart unbound. Vamos aguardar um pouquinho, enquanto isso ele deve estar fazendo o download da zona-raiz. Pronto, já terminou e, como a gente tinha comentado, o tamanho do arquivo da zona-raiz é bastante pequeno, fica em torno aí de 1 ou 2 megabytes. Então, vamos dar uma olhadinha aqui, ver se o Unbound trouxe a zona-raiz. Está aqui, root.zone, um pouco mais de 2 mega de tamanho de arquivo, e muito bem.

Agora, pessoal, a gente pode dar uma olhadinha no conteúdo desse arquivo novo que foi criado, da root.zone. Vamos dar uma espiada pra ver o que tem lá dentro. E está aqui. Apresento pra vocês então a zona-raiz do DNS, que nada mais é do que a lista de todos os domínios de topo existente, incluindo o .br, o .com, o .r, todos os domínios de topo, os que estão mais à direita dos nomes de domínio, estão listados aqui, juntamente com seus servidores de nomes, autoritativos, números IPv4 e IPv6. Está aqui toda a lista, a gente está com mais de 1.200 nomes de domínios de topo cadastrados na zona-raiz. Muito bem. Está aqui ela, já faz parte dos recursos no nosso Unbound, e agora a gente pode passar pra alguns testes de funcionamento do Hyperlocal, ok? Talvez, a gente note alguma melhora sensível no desempenho das consultas.

Vamos lá. Lembrando que a gente fez um teste, que levou sete milissegundos pra resolver um domínio inválido, na nossa máquina sem Hyperlocal, agorinha há pouco, e podemos usar uma comparação aqui, fazer um teste parecido pro recursivo do Google. Algum nome que não existe, nomeqnaoexiste.tldqnaoexiste. Legal. Consultando então o DNS público do Google, a gente levou nove milissegundos pra ter essa resposta, de que esse domínio não existe. Muito bem, guardamos essa informação. Vamos fazer um teste 3 aqui, recursivo do meu provedor. Vamos fazer aqui, vou utilizar um domínio que não existe também, principalmente é importante colocar um TLD que não existe, depois do ponto, e... Ah, apontar aqui na frente o meu roteador, que vai passar isso pro DNS do meu provedor. Vamos ver quanto tempo leva, 14 milissegundos. Legal, o meu provedor levou 14 milissegundos pra resolver um nome que não existe, através de uma resposta nxdomain do servidor-raiz. Legal, agora vamos

finalmente testar o nosso, o nosso Hyperlocal. Vou colocar aqui um dig, nome que não existe, não preciso apontar pra nada, vamos ver quanto tempo levou. Melhorou um pouquinho, melhorou um pouquinho, três milissegundos de tempo de resposta, né? Pode ser que melhore um pouco em alguma máquina de verdade, não numa máquina virtual. Posso fazer um novo teste aqui, qualquer nome que não existe... Opa, dessa vez aqui a gente conseguiu 0 milissegundos. Por quê? Porque ele simplesmente consultou no arquivo que ele já possui da zona-raiz, o root.zone, e verificou que o TLD que eu digitei aqui pra consulta não existe na base, de maneira nenhuma, e me trouxe uma resposta imediata. Então, em termos de performance, essa é a melhora sensível que a gente consegue ver, pessoal, pro Hyperlocal. Lembrando que ele adiciona também um outro benefício, que é uma melhora na resiliência. No caso de falha completa de todos os servidores-raiz disponíveis pro nosso [interrupção no áudio] recursivo, ou uma máquina, um servidor de DNS recursivo configurado com Hyperlocal vai poder fazer essa resolução, independente dos servidores-raiz. Legal?

Então, era isso que a gente queria demonstrar nesse teste, e deixando aqui uma dica de configuração do Firewalld, muito bem elaborada pelo Felipe Padilha, no canal do Youtube dele. Pra quem quiser se aprofundar nisso, não é o objetivo do nosso curso agora, mas pra quem quiser se aprofundar, aqui tem uma sugestão de configuração do Firewalld pra servidor recursivo e melhoria um pouco da segurança, ok?

Então é isso. Agora, a gente vai passar pra próxima parte e voltamos em breve. Grande abraço.

SR. NICOLÁS ANTONIELLO: Olá novamente. Vou tentar falar em portunhol, não riam muito. O que vamos ver agora é como configurar um servidor recursivo, o Bind9, com validação DNSSEC e com Hyperlocal. Algumas explicações já foram feitas pelo Daniel, então o que vamos fazer é... Vamos pulá-las. Então agora vou compartilhar... vou parar minha câmera e vou compartilhar a minha tela para você poder seguir a configuração do BIND. Isso. Vou tentar parar minha câmera. Então, você já tem o VirtualBox, tem duas máquinas virtuais instaladas, criadas, tem uma máquina virtual, Servidor, que vamos utilizar para fazer a instalação do Bind9, a configuração, e uma outra máquina virtual, Cliente, que vamos utilizar para fazer as pesquisas no recursivo.

Então, vamos abrir a máquina virtual Servidor. O primeiro que... Vamos voltar à máquina virtual, chave... O usuário é Luke Skywalker e a senha é icannlab1. Isso. Então, esta é a nossa máquina Servidor. Primeiro, o que vamos fazer é encontrar qual é o endereço IP que foi assignado por nosso roteador ao nosso servidor. Para isso, utilizamos o comando ip addr, e aqui, 10.0.1.43 é o endereço assignado para nosso servidor pelo nosso roteador, é um endereço IP da minha rede local, 10.0.1.43.

Então, agora o seguinte que vamos fazer, vamos utilizar um terminal, uma conexão SSH para acessar nosso servidor e fazer a configuração desse terminal SSH. Isso vai ser para nos facilitar o copy-paste, deste nosso documento, deste nosso guia prático, para poder copiar e pegar os comandos diretamente no terminal. Então, para fazer isso, se nossa máquina tiver Linux ou OS X, basta que você, basta pra você abra um terminal e conecte ao nosso servidor via SSH. Se você estiver utilizando Windows, o que pode fazer é usar um aplicativo cliente SSH, chamado PuTTY, e, mediante esse cliente, acessar o servidor via SSH. Em meu caso, vou utilizar um terminal, porque a minha máquina é OSX. Vou abrir só o terminal, da forma que temos aqui o guia da prática, aqui o meu terminal. Lembra que o endereço atribuído a nosso servidor é 10.0.1.43, então vamos acessar nossa máquina Servidor: ssh @10.0.1.43, vamos acessar como usuário root, yes para que gere fingerprints, e a senha, a mesma senha, icannlab1. Isso. Já acessamos nossa máquina Servidor, aqui você pode ver que é a mesma máquina que estamos conectados, Servidor.

Então, agora o que vamos fazer é começar com a instalação do Bind9. Vamos instalar bind9, vamos instalar bind9utils, vamos instalar a documentação do BIND e vamos instalar dnsutils. Estes pacotes, bind9 é propriamente o servidor, servidor BIND; bind9utils e dnsutils são dois pacotes com aplicativos que vão nos servir de ajuda, ferramentas para poder executar algumas ações. Tem aplicativo dig, tem aplicativo para verificar a configuração do Bind9, tem outros aplicativos para verificar toda a configuração dos distintos arquivos, files de configuração de BIND, e toda a documentação de BIND. Então, vamos instalar primeiro bind9 e bind9utils. Yes, se nos pergunta, respondemos yes. Isso leva uns minutinhos. Acho que inventei uma nova palavra em portunhol, minutinho. Agora, vamos instalar os outros dois pacotes, bind9-doc e dnsutils. Isso, então agora temos BIND instalado. O diretório padrão onde se instala BIND é /etc/bind/. Se olharmos o conteúdo de diretório /etc/bind/, vemos que estão os arquivos named.conf.options e named.conf, estes dois, vão ser os arquivos de configuração de BIND que vamos utilizar hoje para nossa configuração. E tem também outros arquivos, uns exemplos de zona, caso você queira utilizar BIND como servidor autoritativo para sua zona, etc. Mas neste caso, nós vamos utilizar Bind apenas como servidor recursivo, então somente vamos modificar configuração do named.conf.options e do named.conf.

Agora, nosso Ubuntu, por padrão, vem com um Firewall ativado, é este ufw, uncomplicated firewall, mas eu gosto de chamá-lo Ubuntu firewall, vou chamar Ubuntu firewall. Então, o primeiro que vamos fazer é assegurar-nos de que a porta 53, que é a porta que nosso servidor recursivo de DNS utiliza para fazer as pesquisas aos servidores autoritativos, e é também a porta que os clientes utilizam para acessar nosso servidor recursivo, vamos assegurar-nos que a porta 53 está permitido em nosso Firewall. Para isso, executamos o comando ufw allow 53. Isso. Agora, habilitou, atualizou as regras de Firewall para permitir tráfego à porta 53, tanto para IPv4 como para IP versão 6. Nossa prática, por simplicidade, vamos utilizar, mais adiante vamos ver que vamos utilizar só o IP versão 4. Mas se você vai implementar isso em um servidor real, um servidor em produção, a nossa recomendação é que vocês implementem sempre os dois stacks, tanto o IPv4 como o IPv6, tá?

Então, agora vamos iniciar nossa configuração de BIND. Primeira configuração que vamos fazer é uma configuração de servidor recursivo sem validação de DNSSEC e sem Hyperlocal, só um servidor recursivo, sim? Uma coisa interessante é verificar este arquivo, que vem com a instalação padrão de Bind. Esse arquivo contém a informação, traz as informações dos servidores-raiz, os nomes, os endereços dos servidores-raiz, para que o servidor recursivo possa acessar os servidores-raiz, para iniciar a resolução de um nome de domínio. Vamos ver o conteúdo de... Aqui você pode ver que tem todos os servidores autoritativos, para cada um dos servidores-raiz, seu endereço IPv4 e seu endereço IP versão 6. Sim? Aqui, este é L, root server L, que é o root server operado por Icann.

Bom, então agora vamos iniciar, como dizia, vamos iniciar nossa configuração de BIND. Para isso, o primeiro arquivo de configuração que vamos modificar vai ser o arquivo named.conf.options. E para editar, para editar arquivo de configuração, vamos utilizar comando, aplicativo Nano. Então, utilizamos o aplicativo nano named.conf.options, e acessamos o arquivo de configuração named.conf.options. Essa é a configuração padrão que vem com a instalação de BIND, e vamos tentar explicar a configuração que vamos fazer. Então, vamos realizar algumas alterações, algumas ações na configuração sobre este arquivo, e vamos explicar essas ações. Como dizia antes, para simplificar a prática, vamos desabilitar protocolo IP versão 6, somente vamos permitir consultas utilizando IP versão 4. No entanto, nós recomendamos sempre que você, em qualquer servidor DNS recursivo que vá utilizar, implementar em produção, nossa recomendação é que você tenha os protocolos IPv4 e IP versão 6, sim? Sempre conveniente instalar os dois protocolos, de forma que o servidor recursivo, as consultas ao servidor recursivo possam fazer ou ser feitas usando protocolo IP versão 4 ou protocolo IP versão 6. Então, o primeiro que vamos fazer, como dizíamos,

é desabilitar aqui essa linha, desabilitar o protocolo de IP versão 6, para facilitar a prática, porque, em princípio, nós não sabemos se vocês têm IPv6 em sua rede. Então, vamos utilizar só IP versão 4 por facilidade.

Outra coisa que vamos fazer é desabilitar a validação de DNSSEC. BIND, a instalação padrão de BIND, já tem validação de DNSSEC habilitada, por padrão. Então, nós vamos desabilitar. Para desabilitar isso, vamos utilizar configuração dnssec-enable no. Isto, esta configuração desabilita a validação do DNSSEC. E vamos comentar esta linha, esta linha, logo quando chegamos na parte de DNSSEC, de validação de DNSSEC, vamos tentar explicar o que significa isto, mas esta parte, sem validação DNSSEC, comentamos, somente comentamos essa linha.

Agora, também vamos a... Outra coisa que vamos configurar para esta parte é... Vamos configurar isto, duas regras que são de uma lista de acesso para permitir apenas consultas DNS provenientes de dois sítios. Vamos permitir consultas DNS provenientes de nossa rede... Sim? Aqui está indicada a nossa rede, 10.0.1.0/24, ou consultas provenientes do próprio servidor recursivo, localhost. Para que isto? Isto para evitar que o servidor recursivo esteja aberto ao mundo. O que significa aberto ao mundo? Significa que, se vocês não configuram essas duas linhas, o que vai acontecer é que qualquer usuário, qualquer pessoa que tenha acesso a sua rede vai poder utilizar seu servidor recursivo, vai poder enviar consultas ao seu servidor recursivo. Desta maneira, com estas duas linhas de configuração, limitamos a capacidade de fazer consultas ao servidor recursivo somente a localhost, ou seja, o próprio servidor, ou a um dispositivo que esteja dentro de nossa rede. Para o resto, vai estar fechado.

Então, vamos inserir as duas linhas à configuração, isso, e finalmente vamos inserir uma linha para habilitar a recursão. De novo, a instalação padrão de BIND, se vocês não incluem essa linha, de todas as formas, BIND vai ter habilitada a recursão. Nós o colocamos explicitamente para este exercício, para mostrar que efetivamente queremos que o servidor, seja um servidor recursivo e que possa resolver estas pesquisas em forma recursiva, ok?

Bom, então, com isso, com essas modificações, este é o arquivo de configuração, que fica desta maneira que temos aqui, sim? Então agora o que vamos fazer, vamos salvar o arquivo, Ctrl+X, save, yes, e já temos nosso arquivo de configuração named.conf.options, para nosso recursivo, sem DNSSEC e sem Hyperlocal, pronto para testar. Então agora o que vamos fazer é, primeiro, primeiramente, verificar nossa configuração, verificar que não há erros em nossa configuração. Para fazer isso, BIND tem um aplicativo, uma ferramenta que nos permite verificar a configuração. Para isso, utilizamos o comando named-checkconf. Então, uma vez que executamos o comando named-checkconf, se não nos diz nada, se não nos devolve nada, quer dizer, significa que tudo está ok, tudo bem. Se há um erro, vai indicar qual é o erro. Então, verificamos a configuração, configuração está correta. Então, agora vamos reiniciar, reiniciar o serviço de BIND, iniciar... Restart BIND. Para isso, utilizamos o comando service bind9 restart. Isso. Agora BIND deveria haver reiniciado e aplicado a nossa nova configuração.

Então, agora, para fazer os testes, o que vamos fazer é... Vamos utilizar uma segunda, uma outra máquina virtual, que tínhamos instalado, essa, nosso cliente. Vamos iniciar nosso cliente. Aí, enquanto isso, vamos lembrar qual era o endereço IP do nosso servidor. Isso. Era 10.0.1.43, então todas as pesquisas que vamos fazer do cliente a nosso servidor, as vamos dirigir ao endereço 10.0.1.43, que é justamente nosso servidor, este BIND recém-configurado. Aqui temos nossa máquina virtual Cliente, mesmo usuário, Luke Skywalker, icannlab1, ok? Isso. Então, com esse cliente aqui, abrimos um terminal, isso, e aqui estamos em Cliente. Se

queremos ver que efetivamente nosso cliente tem um outro endereço IP assignado, ip addr... Aqui. Nosso roteador atribuiu o endereço IP 10.0.1.88 a nosso cliente.

Então, agora vamos fazer alguns testes sobre o nosso servidor BIND. Para isso, vamos utilizar o mesmo comando dig, que foi explicado por Daniel antes. Então, vamos fazer os mesmos testes que foram feitos por Daniel para Unbound, vamos fazer nós agora para nosso servidor Bind9. Então, se simplesmente executamos nosso comando dig a nosso servidor, endereço 10.0.1.43, efetivamente nosso servidor, aparentemente, está funcionando corretamente. Status: no error, e, como não especificamos um nome de domínio particular, o que nos devolve nosso servidor é a lista dos servidores, de todos os servidores-raiz, que é o que a instalação padrão já tem configurado. Então, agora vamos fazer alguns outros testes, vamos provar, por exemplo, um dig a www.google.com. Aí temos resposta, na seção Answer, nos devolve o registro A, endereço associado a google.com. Vamos a consultar agora por lacnic.net, o registro de MX de lacnic.net, ou seja, queremos conhecer qual é o nome do servidor de correio eletrônico atribuído a lacnic.net. Escrevemos dig a nosso servidor, endereço de nosso servidor, lacnic.net e tipo de registro que queremos consultar, que neste caso é o MX. E aqui, na seção, obtemos dois servidores de correio eletrônico associados ao domínio lacnic.net: o servidor, o nome do servidor de correio mail.lacnic.net e o nome do servidor de correio registro.lacnic.net. Estes são dois servidores de correio associados a esse domínio. E vamos consultar este, agora, por exemplo, o registro quádruplo A (AAAA), endereço IP versão 6, associado ao domínio afrinic. Se bem, nosso servidor não está, está desabilitada a consulta a nosso servidor via IP versão 4, sim, podemos perguntar-lhe, para que nos resolva o registro quádruplo A(AAAA) de um nome de domínio: afrinic.net, registro quádruplo A(AAAA)... Aqui. A seção Answer para o domínio afrinic.net resolveu, e o endereço 2001:42d0:0:200::6 é o endereço IP versão 6, atribuído a afrinic.net. E por último vamos fazer este teste, vamos perguntar a nosso servidor, por um domínio que não exista, por um domínio de primeiro nível que não exista, sim? Então, vamos colocar dominioquenaoexiste... Sim? Para ver o que é que nos devolve. Se olhamos aqui, efetivamente, nosso servidor, isso, pesquisa ao servidor, a consulta ao servidor-raiz, o servidor-raiz nos devolveu que esse domínio não existe e por isso não se está dando status no reader, nos está dando status non existent domain, sim? Este servidor, este domínio que nós consultamos não, efetivamente, não existe. E se olhamos aqui embaixo, também temos o tempo que consumiu esta consulta. Esta pesquisa foi... Esse teste foi por um domínio de primeiro nível, que não existe, ou seja, que somente nosso servidor consultou ao servidor-raiz, obteve a resposta non existent domain e nos devolveu a nós, ao cliente, a resposta. Tudo isso, tudo isso consumiu 600 milissegundos, sim? Recordemos este tempo para a parte final da prática, quando estaremos Hyperlocal, para ver justamente como muda este tempo, quando temos uma cópia da zona-raiz instalada localmente, em nosso servidor recursivo, sim?

Bom, um outro teste que podemos fazer é enviar nossas consultas, mas em vez de enviar a consulta por www.google.com a nosso servidor recursivo, vamos fazer a consulta a um servidor recursivo público de Google, que tem o endereço direto: 8.8.8.8. E vemos, tempo de resposta muito menor. Isto provavelmente se deve a que Google tem um... Meu ISP, meu provedor de acesso à internet, ou alguma rede esteja bem mais perto, em termos de rede, à minha rede, tem um servidor, um cache, um servidor recursivo de Google e um servidor autoritativo, provavelmente, de Google, muito mais próximo. Então, essa é a razão pela qual o tempo de resposta é muito menor. Se, por exemplo, tentamos fazer a mesma consulta ao servidor de Google, mas agora por... Por exemplo, vamos testar: lacnic... www.icann.org, por exemplo. Juntamos ao servidor recursivo de Google, pelo registro A de icann.org, aí demorou, o tempo de resposta é de 162 milissegundos, é o que demorou nosso, o servidor de Google, nesse caso, recursivo do Google, em

resolver o registro A do domínio icann... www.icann.org, foi mais ou menos, aproximadamente 162 milissegundos, sim?

E, por último, outro teste que podemos fazer é tentar verificar o tempo de resposta dos servidores-raiz. Para isso, podemos utilizar este comando, de forma igual ao que Daniel explicou antes. Vamos utilizar este comando, dig, vamos consultar, por exemplo, o servidor autoritativo, diretamente vamos enviar a consulta ao servidor autoritativo administrado por ICANN, ao root server L. Vamos pedir-lhe id.server e os registros ch txt. Aqui vemos o tempo de resposta desta consulta, diretamente ao servidor autoritativo L, ao servidor autoritativo administrado por Icann, de quatro milissegundos. É um tempo muito baixo. A razão desse tempo muito baixo, tão baixo, é que em meu ISP, meu provedor de acesso à internet, tem uma cópia, uma cópia do servidor administrado por Icann, tem uma cópia do root L em meu ISP. Então, o tempo de resposta é muito rápido. Se, por exemplo, em vez de consultar ao servidor, enviar a consulta ao servidor autoritativo L, enviamos a consulta ao servidor autoritativo B, vemos que o tempo de resposta é muito mais alto, porque não há uma cópia do servidor autoritativo B, do root server B, em meu ISP, nem está tão perto da minha rede, sim?

Então, agora, finalmente, é o último teste que vamos fazer com a configuração atual de nosso servidor recursivo, é tentar fazer uma consulta a uma... Por um domínio que está atribuído por... Com DNSSEC, mas lembre que nosso servidor não está fazendo verificação de DNSSEC. Então, para isso vamos fazer uma consulta ao domínio dnssec-failed.org, que está atribuído com DNSSEC, mas essa assinatura é falsa. Então, se meu servidor estivesse validando DNSSEC, deveria devolver um erro, ser failed. Como não está verificando DNSSEC, nosso servidor recursivo, o que vai acontecer é que deveria resolvê-lo corretamente, porque não vai verificar a assinatura de DNSSEC. Então... dig dnssec-failed.org, temos que dirigir a pesquisa a nosso servidor, 10.0.1.43, dnssec-failed.org. E aqui na seção Answer, efetivamente, nos devolve o endereço IPv4 associado a dnssec-failed.org, 69.252.80.75. E em status vemos no error. Por quê? Porque se vem uma assinatura incorreta, como nosso servidor recursivo não está verificando DNSSEC, não tem nem forma de verificar que a assinatura disso, DNSSEC, não é correta, então o único que pode fazer é devolver-nos o resultado.

Então agora o que vamos fazer é modificar a configuração do nosso servidor recursivo para habilitar a validação de DNSSEC. Então, para fazer isso, voltemos, vamos ao terminal com nosso servidor recursivo e vamos fazer uma modificação no arquivo de configuração named.conf.options, mesmo arquivo que já havíamos configurado. E a modificação é muito simples, muito fácil. Colocamos dnssec-enable yes para habilitar validação de DNSSEC, e configuramos dnssec-validation auto. Que é dnssec-validation auto? O que vai acontecer com dnssec-validation auto é que a instalação de Bind, se você tem isto configurado, dnssec-validation auto, automaticamente vai manter, vai buscar e vai armazenar localmente a versão atual da assinatura pública da raiz. Se você não tem dnssec-validation auto, o que você vai ter que fazer é... Você vai ter que, de forma manual, obter a assinatura da zona... da chave pública da assinatura da zona-raiz, e armazenar localmente, de forma manual. Mas a recomendação é ter dnssec-validation auto, de forma que, se em algum momento, num futuro, se a assinatura, a chave que se usa para assinar a zona-raiz do DNS, faz um roll over, automaticamente nosso servidor recursivo vai obter essa nova assinatura e vai armazenar localmente. Essa nova chave pública, vai armazenar localmente, você não vai ter que, manualmente, lembrar de modificar a assinatura pública, com a última versão. Então, apenas com essas duas linhas de configuração, habilitamos a validação de DNSSEC, Ctrl+X, yes. Agora, vamos novamente utilizar o comando para verificar... nosso arquivo de configuração. Se não retornar nada, lembra que está tudo bem. E, finalmente, vamos reiniciar, restart BIND.

Isso, ok. Então, agora nosso servidor recursivo está validando, deveria estar validando DNSSEC, tá? Certo? Para isso vamos realizar alguns testes. Então, voltemos ao nosso cliente, e agora, desde nosso cliente, podemos realizar algumas consultas novamente ao nosso servidor, ao nosso servidor recursivo. Vamos provar agora, fazer a consulta pelo registro A do NIC.br, mas vamos pedir-lhe que nos mostre a informação de DNSSEC, se NIC.br tem assinado seus registros com DNSSEC. Deveria devolver-nos a chave pública de registro A, neste caso. Neste caso, dnssec, ok. Esta opção, dnssec, nos mostra a informação de DNSSEC associada ao nome de domínio nic.br, e esta opção +multi, o que faz é mostrar-nos em forma mais humanamente legível, ou mais fácil para nós humanos, para ler, para poder ler corretamente a informação. Então, aqui vemos que, na seção Answer, efetivamente, nos devolve o registro A de nic.br, e também nos devolve o registro rrsig, que, entre outras coisas, contém a assinatura do registro A, associado ao nome de domínio nic.br. Sim, a informação de DNSSEC, associada a esse registro. Em particular, se você lembra, há três registros principalmente associados a DNSSEC, que são o dnskey, o registro DS e o registro RRSIG. Podemos fazer a consulta DNS por esses três registros, associados a nic.br: dnskey... Aqui está o registro de dnskey, associado ao nome de domínio nic.br. Podemos consultar pelo registro DS. Aqui está o registro DS, associado ao nome de domínio nic.br. E podemos consultar o registro RRSIG, associado ao nome de domínio nic.br, e, bom, aqui vemos que temos dois registros RRSIG associados ao domínio nic.br, em particular o RRSIG do registro A, o RRSIG do registro dnskey e o RRSIG do registro DS.

Por último, vamos fazer o teste que havíamos feito antes, agora com validação de DNSSEC habilitada, vamos pedir-lhe que nos resolva o domínio dnssec-failed.org. Então, fazemos o dig ao nosso servidor e lhe perguntamos pelo registro A de dnssec-failed.org. E notem que agora, o que acontece? Agora, como está validando DNSSEC e dnssec-failed.org está assinado, intencionalmente assinado com uma assinatura falsa, digamos, que não verifica DNSSEC, nosso servidor justamente nos devolve no status, nos devolve SERVFAIL, que significa que não verificou a assinatura, neste caso, de DNSSEC, sim? Pelo qual, à diferença do teste que havíamos feito antes, sem validação de DNSSEC, aí então nos devolvia o registro A. Neste caso, como não verifica a assinatura, não nos devolve o registro A, nos devolve um erro, indicando-nos justamente que essa assinatura não é correta, sim?

Agora, o que acontece se, neste caso, que eu sei que está falhando a validação de dnssec-failed.org, o administrador, o administrador de dnssec-failed.org liga pra mim e me diz: Alô, tenho um problema, estou tendo um problema com a assinatura do meu domínio dnssec-failed.org, mas vou demorar uns minutinhos para resolver o problema. Se você pode gerar uma exceção pra meu domínio, para que as consultas por dnssec-failed.org sejam respondidas pelo seu servidor recursivo. Então, como podemos fazer para criar uma exceção de DNSSEC no BIND? Para isso, existe algo chamado âncora de confiança negativa, NTA. NTA, as âncoras de confiança negativa podem ser usadas para, justamente, para mitigar essas faixas de variação de DNSSEC, desativando essa validação, para domínios específicos, durante um tempo específico. O tempo padrão é uma hora, ou seja, se eu gero, crio uma exceção e não específico um tempo, a exceção vai durar uma hora. Durante uma hora, vou ter a exceção. Passada essa hora, vou voltar à configuração padrão, sem exceção. Sim?

Então, para visualizar isso, vamos gerar no nosso servidor uma exceção para o domínio dnssec-failed.org. Para isso, vamos a... Voltemos ao nosso servidor, sim? E vamos utilizar, para o caso, no caso do BIND, para criar essa exceção NTA, essa âncora de confiança negativa, usamos o comando rndc nta, seguido pelo nome do domínio ao qual queremos abrir a exceção. Vamos gerar essa exceção em nosso servidor. Sim? Aqui. Negative trust anchor added: dnssec-failed.org/_default, expires e uma hora a partir de agora. Tá? Tá bem? Então, agora, que acontece se acessamos o seu cliente e voltamos a fazer mesma consulta, sim? Que estava dando SERVFAIL, porque a assinatura não verificava. Agora, no error, sim? Mesma consulta, pelo

registro A associado ao dnssec-failed.org. Como nosso servidor recursivo tem uma exceção para esse nome de domínio, o que vai fazer nosso servidor recursivo é: não vai validar DNSSEC, não vai verificar DNSSEC. Como não verifica DNSSEC, o status é no error e efetivamente nos devolve o endereço IPv4 associado ao nome do domínio dnssec-failed.org. Então, este é o mecanismo, a ferramenta para gerar uma âncora de confiança, para criar uma exceção com âncora de confiança negativa. Bem.

Aqui, vocês têm uma informação adicional. Este é o tempo de vida padrão de um NTA, de um negative trust anchor. É de uma hora, como havíamos mencionado, embora, por padrão, vai fazer uma pesquisa, automaticamente vai fazer uma pesquisa na zona, a cada cinco minutos. Isso é para verificar se a zona agora é válida corretamente. Caso seja válida corretamente, vai expirar automaticamente, não vai esperar uma hora, vai expirar antes. Faz pesquisa a cada cinco minutos, se detecta que agora valida, o que faz automaticamente é: expira a exceção e começa a validar. Se não, se não, o tempo de vida padrão, como mencionamos, é de uma hora. E você também pode usar o parâmetro lifetime duration para especificar um tempo de vida diferente ao tempo padrão, um tempo de vida diferente uma hora, e você vai poder por um valor máximo permitido de uma semana, nessa exceção NTA, sim?

Bom, finalmente você tem um comando útil para visualizar o servidor, as exceções que você tem atribuídas, que é o comando rndc nta-dump. Aqui, você pode ver que, para o nome de domínio dnssec-failed.org há uma exceção que expira dentro de... Já é menos de uma hora, sim? E aqui me indica, se houvessem mais exceções, se você tem mais exceções, este comando vai listar todas as exceções que você tem em seu servidor recursivo, sim? Tá bem?

Bom. Então, agora, finalmente nos falta a última parte, que é a implementação de Hyperlocal em nosso servidor. Daniel já... Esta parte já foi explicada pelo Daniel previamente, então vamos ir diretamente à configuração do BIND para Hyperlocal. Antes, vamos... Antes dessa implementação, vamos fazer novamente um teste, desde nosso cliente ao nosso servidor, vamos perguntar por... pesquisar por um domínio, vamos enviar uma consulta ao nosso servidor por um domínio de primeiro nível que não exista. Assim, dessa maneira, vamos verificar o tempo de resposta para esse domínio, por exemplo, esse que escrevemos, qualquer domínio de primeiro nível, que não exista, sim? Ok? Vamos obter um non-existent domain, NXDOMAIN, status de domínio inexistente, e deveríamos obter também o tempo de resposta. Aqui, efetivamente, esse domínio não existe, temos o status NXDOMAIN, e o tempo de resposta, 476 milissegundos. Vamos lembrar este, anotar esse tempo de resposta para mais adiante, sim? Então, o objetivo do Hyperlocal é ter uma cópia da informação de toda a zona-raiz em nosso servidor recursivo, de forma que nosso servidor recursivo não tenha que fazer a consulta a um servidor-raiz, senão que diretamente acessa o arquivo local, que tem a cópia do servidor-raiz, e obtém a informação dos domínios de primeiro nível, diretamente desse arquivo, sem necessidade de fazer a consulta. Então, o tempo de resposta deveria ser de menos de dois milissegundos, ou zero milissegundos, porque diretamente obtém a informação de seu próprio arquivo, e não tem que sair a buscar, pesquisar, sim?

Então, vamos... Como fazemos a configuração de Hyperlocal em nosso servidor BIND? Vamos ao nosso servidor BIND. E o que vamos fazer, para configurar Hyperlocal em nosso servidor, vamos modificar dois arquivos de configuração. Vamos a modificar arquivo de configuração named.conf.options, e vamos modificar um outro, mais um arquivo de configuração, o named.conf, que é um que não configuramos. Primeiramente, então, vamos acessar o arquivo named.conf.options, para fazer algumas modificações de configuração, de forma de habilitar o Hyperlocal. Para isso, voltamos a utilizar o editor Nano. Agora, nosso arquivo, named.conf.options. E a configuração que vamos modificar aqui, simplesmente o que vamos fazer é... Porque vamos especificar em outro, no outro arquivo de configuração, vamos tirar esta configuração

daqui, da parte de options. O que contém o arquivo named.conf.options são as opções de configuração. Então, quando somente tínhamos o servidor recursivo, este validando DNSSEC, toda a configuração está aqui. Só com a manipulação desse arquivo de configuração, já teremos todo o necessário. Agora, vamos deixar as opções, somente as opções nesse arquivo, e o resto da configuração, vamos realizar no outro arquivo, no named.conf, sim? No named.conf. Então, a parte de recursão, tiramos daqui e vamos pôr no outro arquivo. Essa é a única modificação que vamos fazer nesse arquivo. Então, salvamos com Ctrl+X, yes, salvamos a configuração e agora o que vamos fazer é editar a configuração do outro arquivo, de named.conf, sim?

Então, utilizando o mesmo editor, o Nano, agora editamos arquivo named.conf. E nesse arquivo, sim, vamos fazer algumas mudanças na configuração. Esta é a configuração padrão do nosso arquivo named.conf, que vocês, como podem ver, aqui inclui os outros três arquivos de configuração: em particular o named.conf.options, que acabamos de modificar agora; o named.conf.local, que, se vocês visualizarem o conteúdo, não vai ter este... não vai ter nada; e este outro arquivo de configuração, o named.conf.default-zones, que contém a informação das zonas por padrão, que vão conhecer nosso servidor recursivo... Como nós vamos definir uma nova visão para poder habilitar Hyperlocal nesse arquivo de configuração, o que vamos fazer é, o primeiro que vamos fazer é comentar este arquivo, para que não seja incluído na configuração, quando reiniciemos BIND, e leia novamente a configuração. Então, vamos comentar, não vamos usar mais esse arquivo, sim?

Agora, vamos gerar a configuração para ter uma cópia local da zona-raiz, sim? Para isso, o que vamos inserir toda esta configuração que estamos vendo aqui. Antes de inserir essa configuração, vamos tratar de explicar um pouco de que se trata. Então, esta primeira parte, o que estamos fazendo aqui é criando algo que se chama visão, sim? Visão para zona-raiz. Primeiramente, criamos a vista, a visão, para a zona-raiz. Isto se faz com este comando, view root, a vista para, a visão para a zona-raiz. Indicamos quais recursivos vão poder usar nossa cópia local da raiz. Como nós vamos... temos um só servidor recursivo, sim? Vamos dizer que o único servidor que vai poder usar essa cópia é o localhost, o próprio servidor recursivo, ou seja, é uma cópia que somente este servidor vai poder utilizar. Isto se pode ser modificado caso vocês tenham vários servidores recursivos e só queiram que um desses servidores recursivos tenha a cópia da raiz, Hyperlocal, configuram só em um, e os outros servidores, os podem habilitar para que venham a consultar este servidor no lugar de ir consultar um servidor-raiz, sim? Mas neste caso, o único que vai poder consultar vai ser o localhost. Então usamos o match-clients, localhost, e logo definimos a parte correspondente à zona-raiz, e basicamente os masters, que são os servidores devido os quais se vai poder, utilizando o protocolo de transferência da zona-raiz, o xfr, se vai poder trazer a cópia e manter atualizada a cópia dessa zona-raiz. E depois, vamos criar outra visão, para atender consultas recursivas, sim? Esta é a configuração para nosso servidor, nossa nova configuração para servidor recursivo, sim? Este... Bom, aí aqui temos o mesmo que tínhamos em named.conf.options, dnssec-enable yes, dnssec-validation auto, permitir recursão somente do próprio servidor ou do cliente de nossa rede, sim? Habilitar explicitamente a recursão, e aqui indicamos que, para resolver a raiz, usaremos a zona local. Não vamos ir consultar nosso servidor recursivo, não vai consultar nenhum servidor autoritativo da raiz, sendo que vai utilizar o arquivo local, a cópia que se transfere destes servidores, este... utilizando o protocolo xfr, que a vai armazenar em este arquivo, rootzone.db. O rootzone.db vai ser o arquivo local que mantenha a cópia atualizada da zona-raiz. E aqui estamos dizendo que qualquer consulta por domínios de primeiro nível, ou seja, qualquer consulta na zona-raiz, tem que fazer uma consulta ao arquivo local, ok?

Então, vamos copiar esta configuração e vamos inserir a configuração em nosso servidor, nosso arquivo de configuração named.conf, em nosso servidor recursivo. Salvamos a configuração, Ctrl+X, yes. Agora, como

sempre, vamos verificar que a configuração, as modificações de todos os arquivos de configuração que fizemos não contêm erros. Para isso, utilizamos o comando named-checkconf. Não há erros, não devolveu nada. Se não retornou nada, está tudo bem. Agora, o que falta? Reiniciar o serviço de BIND: service bind9 restart. Pronto. Então, agora nosso servidor deveria estar, nosso servidor recursivo tem validação de DNSSEC mais Hyperlocal.

Como podemos verificar que temos... que reiniciou? Que nosso servidor BIND reiniciou corretamente? Uma coisa interessante que podemos fazer é verificar o arquivo de syslog, sim? Utilizando o comando tail, podemos verificar o syslog. Se vocês utilizarem o comando tail, desta maneira... O que vai fazer este comando, tail -f, é mostrar-nos a última parte do syslog. Com Ctrl+C saímos dessa visualização, e o que temos aqui é a última parte do que se registrou no syslog, quando reiniciei o BIND, aqui. Se reparem, completou a transferência da zona-raiz, sim? E o que vamos fazer agora é verificar... Aqui diz transfer status: success, transfer completed, sim? O que vamos tentar fazer agora é fazer uma verificação do nosso servidor, com Hyperlocal, e ver a diferença no tempo de resposta, quando fazemos uma consulta por um domínio de primeiro nível, sim?

Antes disso, vamos verificar que nosso arquivo local, com a cópia da zona-raiz, se criou corretamente, ou seja, que temos um arquivo rootzone.db. Para isso, listamos o conteúdo do diretório... Este diretório: /cache/bind/, sim? E verificamos que se criou corretamente o arquivo, a base de dados, a database do rootzone: ls... Aqui, efetivamente vemos que se criou corretamente, ou seja, que se transferiu corretamente a zona-raiz, e temos a base de dados do arquivo criado com a zona-raiz. Aqui veem o tamanho, não muito grande, mas, bom, significativo da base de dados da zona-raiz, da cópia da zona-raiz.

Então, o que vamos fazer agora é fazer, finalmente, fazer o teste, esse mesmo teste que havíamos feito hoje. Para isso, voltemos a nosso cliente, sim? E recordem que, antes de ter Hyperlocal, nosso cliente tinha... Quando fazíamos uma consulta por um domínio de primeiro nível, que não existia, nosso servidor recursivo ia consultar o servidor-raiz, o servidor-raiz ia devolver um non-existent domain, um status NXDOMAIN, sim? E tudo isso nos levou da ordem de 476 milissegundos. Agora, temos uma cópia local do servidor-raiz, então, se perguntamos por um domínio de primeiro nível, em vez de sair para procurá-lo em um servidor-raiz, o vai consultar diretamente no arquivo local. Então, o tempo de resposta deveria ser significativamente menor. Voltamos executar uma consulta ao nosso servidor, por um domínio qualquer, não existente, e aqui vem o tempo resposta de quatro milissegundos, sim? Esse tempo de resposta, mesmo se provamos a... Em vez de fazer a consulta de um cliente, fazemos desde o próprio servidor-raiz, se fazemos um dig @localhost por um domínio de primeiro nível não existente, sim? Notem que o tempo de resposta aqui é 0 milissegundos, diretamente. Olha o arquivo local, com a cópia da raiz, não existe esse domínio, diretamente me põe domínio inexistente. Sim? Pelo contrário, antes de ter Hyperlocal, antes de ter uma cópia do servidor-raiz, uma cópia local do servidor-raiz, o tempo era muitíssimo mais significativo, sim? Bom, esta é a comparação dos tempos obtidos agora com os que obtivemos quando não tínhamos Hyperlocal configurado.

Bom, até aqui está a configuração do nosso BIND, então, finalmente, temos nosso servidor Bind9, recursivo, com validação de DNSSEC e com Hyperlocal.

Espero que lhes tenha agradado a apresentação e que tenham podido segui-la e replicá-la.

Bom, nos vemos então em um momento para responder dúvidas, para consultas ou para comentários. Muito obrigado, até logo.

SR. EDUARDO BARASAL MORALES: Bom, muito esclarecedor aí. Muito obrigado Nicolás, Daniel. Foi realmente muito interessante tudo que vocês apresentaram.

Antes de a gente ir para a parte de perguntas e para a parte de apresentações extras, fazer os pequenos comentários, eu queria chamar agora o formulário de avaliação. Agora a gente gostaria que vocês preenchessem esse formulário de avaliação. É um formulário que vai dizer se ele é bom ou se está ruim toda essa transmissão que a gente fez, todo esse evento que a gente está aí trazendo para vocês. Então, se puderem preencher o formulário de avaliação, tem um QR Code que a gente está colocando aí na tela. Isso nos ajuda muito a saber o que a gente deve fazer para o futuro, o que a gente pode melhorar. Então, por favor, preencham esse formulário de avaliação, são duas perguntinhas, é coisa simples. Então é uma nota de 0 a 10, e o que a gente pode melhorar. Se você quer deixar algum comentário, ou quiser até mandar alguma mensagem aí para o Daniel Fink, para o Nicolás, o que você ali acha que eles podem melhorar também na questão da didática. A gente passa para eles também.

E lembrar também, quem quiser o certificado de participação dessa live, a gente está colando no chat - então aí é diferente - um outro link relacionado ao formulário de inscrição da live. Então aqui é um formulário que você vai preencher para ganhar o certificado. Então quem quiser o certificado preenche esse outro formulário. É até às 2h da tarde. Depois disso, a gente vai fechar e não vai ter como você ganhar o certificado da live. É só para quem está assistindo ao vivo.

Bom, vamos começar aí com as perguntas, porque Daniel e o Nicolás já estão ansiosos para aparecer. Então eu vou começar aí fazendo a perguntinha para o Daniel.

Daniel, o pessoal está querendo saber aí da possibilidade de ter um servidor cópia do root. Então, o Paulo Júnior de Andrade perguntou isso daí, como que ele faz para conseguir ali uma cópia do root. Fica à vontade.

SR. DANIEL FINK: Valeu! Valeu, pessoal! Obrigado, Eduardo.

Antes de responder, eu queria agradecer demais aí, tirar o chapéu para vocês por essa oportunidade. Foi bem bacana fazer essa prática. E agradecer também ao pessoal que está assistindo, teve muita ajuda, muita colaboração, muitas perguntas aí. Os próprios colegas já responderam. Então obrigado mesmo.

Queria agradecer também para o pessoal da Solintel, Lacier, o João Bertoncini, que lá no ano passado, quando a gente começou a elaborar essa prática, eles deram uma tremenda força, pessoal 100%. E também quando a gente terminou o caderno de práticas, o Douglas Fischer e o Rubens deram a maior força também, com várias dicas, inclusive o Douglas Fischer me disse: "Ó, se você manter o firewall desconfigurado e não ensinar a fechar ele, a gente vai matar você."

Então, pessoal, por isso que a gente colocou tanto alerta, tanta dica para fazer essa prática mesmo em casa, a parte do firewall a gente deixa para uma próxima, mas já teve bastante colaboração por aqui também.

Bom, sobre a primeira pergunta, é possível ter, além do Hyperlocal, vocês podem também se candidatar a ter uma cópia de um servidor-raiz físico mesmo. Existe um programa que a gente faz na Icann de enviar uma máquina para o provedor de vocês, que a gente chama de IMRS, o servidor-raiz gerenciado pela Icann. Então vocês podem alojar uma instância do servidor-raiz. Para fazer isso tem um processo, começa por um mandar e-mail para mim ou para o Nicolás, fazendo a solicitação. A gente passa todas as informações para vocês. E, dentro desse processo, vocês só precisam adquirir um servidor, só adquirir uma

máquina. E aí a engenharia da Icann faz toda a configuração. Vocês podem ter essa máquina real dentro do Data Center de vocês, além de ter o Hyperlocal, né? O Hyperlocal não tem nenhum custo. Isso que a gente explicou aqui, vocês podem fazer imediatamente.

SRA. ANDREA ERINA KOMO: Oi, pessoal! Bem, obrigada, Daniel. Agora eu queria fazer uma pergunta aqui para o Nicolás. O Tiago(F) Sanchez mandou para a gente, né? "O palestrante afirma que essa prática não serve para ser implementada em servidores que se encontram em produção. Por que isso?" Então a gente já tinha falado, né, vocês tinham enfatizado isso, mas eu acho que é bom comentar aí de novo para o pessoal ao vivo e falar os pontos que faltam e por que não pode estar em produção esse tutorial que vocês passaram. Por favor, Nicolás, fica à vontade.

SR. NICOLÁS ANTONIELLO: Ah, bom dia para todos. Creio que a razão principal é porque você tem que ter em conta, além da configuração que nós utilizamos como exemplo, você tem que ter em consideração outra configuração de segurança para [ininteligível] de segurança, configuração de segurança no mesmo servidor DNS. Sim? Tem que considerar qual é a versão do servidor que você vai utilizar. Por exemplo, se você vai utilizar o BIND, você tem várias possíveis versões para utilizar. E você tem que eleger, dependendo se você quiser, por exemplo, se você quer estabilidade, quer uma versão bem testada, tem que utilizar determinada versão de BIND. Se você quer ter as últimas features, você tem que utilizar uma outra versão.

Então a prática, essa prática está pensada para que você faça testes. Tá? Você ganhe experiência com BIND, com Unbound... Mas se você quer ativar essa produção, nossa recomendação é que você pratique muito primeiro. E, depois, considere essas questões de segurança, essas questões de estabilidade e decida qual é a versão de BIND que quer utilizar, em que tipo de servidor vai utilizar. Se vai colocar a versão sobre o mesmo servidor, se vai utilizar algum hiper [ininteligível], se vai usar Ncast, boas práticas de configuração da rede, BGP... se você utilizar [ininteligível] tem que considerar boas práticas de segurança para essa configuração etc. Essa é a razão principal.

Se você já tem um servidor em produção, essa configuração é possível utilizar em produção sem problema. Você pode [ininteligível] com essa configuração, ou a configuração que for necessária de acordo com a versão do provedor que você tenha... você pode usar essa configuração para agregar, para [ininteligível] DNSSEC e para [ininteligível] Hyperlocal, tá?

SR. EDUARDO BARASAL MORALES: Muito bom, Nicolás. Realmente, eu acho que a questão aqui é a segurança. Porque vocês mostraram como fazer, mas não dá para a gente entrar em todos os requisitos de segurança nesse tutorial aqui, que foram só três horas. E se a gente falar dos inúmeros ataques que podem surgir em DNS Recursivo, isso também tomaria ali muito mais tempo. Então aqui foi um começo de conversa, vamos dizer assim, né?

E para aqueles que assistiram ontem também a live lá da Josiane, ela falou também sobre questões de segurança nos DNSs Recursivos. Então chega a ser uma coisa que adiciona na fala que vocês estão fazendo agora.

Então vamos lá para a próxima pergunta? Então a próxima pergunta do Ivanilson Pacheco. "Não sei se já foi comentado, o ideal é usar o nosso DNS nos clientes? É correto isso? Pergunto porque um determinado consultor falou para o chefe dele que não recomenda usar o próprio DNS nos clientes." Então ele está pensando num DNS Recursivo para os clientes dele. Ele quer saber se tem vantagens ou desvantagens de ter isso daí para os próprios clientes? E aí eu queria chamar você, Daniel, para responder essa pergunta.

SR. DANIEL FINK: Tá legal! Bom, a grande vantagem que eu acho é física mesmo. Ter um DNS Recursivo próximo dos clientes vai fazer com que a resposta chegue mais cedo, né? Então, a gente tem um ganho de performance aqui. Quando o DNS Recursivo está dentro do provedor, está na rede do provedor, ele praticamente está na rede local do cliente. Então é o ponto mais próximo, eu acho que é o ponto mais estratégico para ter o servidor recursivo. Então a gente tem ganho de performance sim, né? Mas tem alguns poréns, tem alguns mas aí.

Colega nosso da Icann lá de Los Angeles costuma dizer: Não se instala um DNS Recursivo e vai embora. Não se esquece dele. Tem que instalar ele bem, tem que configurar ele bem, tem que monitorar ele muito bem, tem que ficar cuidando. Aí, sim, a gente tem benefício de ter ele dentro da nossa rede.

É melhor utilizar um DNS público para os clientes do que ter um DNS mal configurado, né? Eu acho que é isso que tem que ficar. Ok?

SRA. ANDREA ERINA KOMO: Obrigada, Daniel. Seguindo aqui nas perguntas. A próxima eu selecionei aqui do Johnny P(F). Eu vou dar uma reformulada aqui na pergunta.

Ele pergunta, no caso, a resposta do DNS, por quanto tempo deveria ficar no cache? É uma boa prática em relação a esse tempo?

Nicolás, quer comentar sobre isso, por favor?

SR. NICOLÁS ANTONIELLO: Sim. Vou colocar um chapéu para estar em sintonia com o Daniel.

Uma boa pergunta. O que acontece é que normalmente o tempo que vai ficar um cache, uma resposta é especificado na resposta no TTL, a resposta de servidor autoritativo. Você não tem que configurar manual, não é necessário que você configure manualmente quanto tempo vá ficar essa resposta no cache. Cache vai receber a resposta do autoritativo, vai olhar o TTL e vai ficar em cache esse tempo. Quando esse tempo expirar isso vai... vai sair do cache. E se outro cliente fizer a mesma consulta vai voltar a consultar autoritativo, vai voltar a receber TTL e vai voltar a ficar no cache.

Então não é algo que realmente você tenha que preocupar-se, que procurar configurar esse tempo. A recomendação é respeitar o TTL que provém do autoritativo. Tá?

SR. EDUARDO BARASAL MORALES: Perfeito, Nicolás. Só complementando ali uma fala do Daniel. Lembrando que vantagem não é só o tempo de resposta, de você estar com o DNS Recursivo mais próximo. O DNS Recursivo é um cache, né? Como você mesmo falou, Nicolás, então ele guarda uma parte da informação de já descoberta que ele já fez. Então se alguém perguntar antes, aquilo lá ele já responde mais rápido ainda, ele nem vai atrás da informação. Então você tem esse ganho também de vantagem.

Bom, vamos fazer aí uma pergunta também vinda aí do Johnny(F) e vinda também do Ivanilson para você, Daniel. Ele comentou aí: "Acho importante frisar os tópicos depois dos itens que devem ser revistos pelos provedores, para colocar em produção, porque vai ter muita gente que vai fazer aí o tutorial dando um Ctrl+C e Ctrl+V." E já puxo a próxima pergunta do Ivanilson, que ele fala assim: Se tem algum curso focado em boas práticas de DNS, algum bom conteúdo, alguma coisa aí que eles podem continuar acompanhando os estudos nesse quesito aí de DNS. E aí eu acho que já é legal de você comentar que o Icann também faz umas lives, né?

Então, manda bala, Daniel.

SR. DANIEL FINK: Tá bom, beleza! Muito bem lembrado a questão do cache também, Eduardo, obrigado.

Pois é, esse é um primeiro curso, e a ideia aqui era fazer amigos. Então, o nosso e-mail está nas... a gente está nas redes sociais também, vocês podem encontrar a gente facilmente. Mandem o que vocês precisam. O que vocês não encontrarem em cursos, a gente customiza para vocês, a gente faz uma outra live, a gente faz um bate-papo. A gente promove eventos toda hora pela Icann, e para ser bem sincero essa é uma das primeiras iniciativas que a gente está fazendo com um tema superprático, tá? Abrindo o terminal e mostrando como é que se faz, e a gente adorou o feedback de vocês. Muita coisa que vocês trouxeram, a gente pode complementar no nosso curso. E se vocês toparem o desafio, vamos fazer, vamos tentar fazer uma segunda live com alguma coisa mais próxima da produção, a gente complementa e marcamos. Acho que o importante é ficar em contato. E a gente pode evoluir por aí. O que vocês acham? Está combinado? Mas mandem feedback, mandem sugestões, entrem em contato, deem um alô para a gente por e-mail, pelo LinkedIn, onde vocês quiserem, e a gente vai construindo. Pode ser, pessoal? Obrigado aí.

SRA. ANDREA ERINA KOMO: Bem, seguindo aqui, a próxima pergunta que eu selecionei aqui foi do Rafael. Coloco aqui: "Vendo que há muitos especialistas de DNS aqui, né? Uma pergunta: BIND ou Unbound?" Então, se puderem comentar um pouquinho aí os pontos positivos de cada um nos diversos ambientes. Por favor, Nicolás.

SR. NICOLÁS ANTONIELLO: Uma boa pergunta.

Acho que você tem sempre que utilizar o que você tiver mais conveniente. Depende da experiência que você tem. Se você tem uma experiência com BIND é melhor utilizar BIND. Se tem experiência com Unbound, melhor utilizar Unbound. Tendo em conta que Unbound é somente para servidor recursivo. BIND pode utilizar como recursivo ou como autoritativo.

O que tem que ter sempre em conta, creio eu, acho, é que se você não se sente seguro é melhor não utilizar nenhuma versão. Melhor ganhar experiência, testar, praticar e depois, depois disso, decidir, de acordo com a sua experiência, a sua preferência de configuração, qual deles você vê mais... mais amigável para configurar e usar essa versão. Sim? Tá bom?

SR. DANIEL FINK: Posso complementar um pouquinho? Tem um vídeo no site do Brasil Peering Forum. Tem uma live lá do Fernando Frediani, do Douglas Fischer, do Ayub e do Rubens. Eles falam muita coisa bacana. Uma delas é... destacam que o Unbound, ele só faz recursivo. Ele é um software só para o servidor recursivo, então ele é mais focado. O BIND faz o autoritativo também. E o Rubens comenta lá que também tem uma taxa de erros, de falhas no software que o Unbound tem uma taxa menor do que do BIND de vulnerabilidades. Só uma observação técnica, mas os dois softwares são superpopulares. É isso que o Nicolás falou, usa o que você gosta mais, o que você conhece mais.

SR. EDUARDO BARASAL MORALES: É, eu acho que essa ideia de falar: use o que você sabe mais é melhor, né? Porque se você tem um conhecimento de como a ferramenta funciona, você consegue ali se precaver de qualquer problema ali de segurança, que aí a gente já ressaltou várias vezes que não dá para dar um Ctrl+C e Ctrl+V nesse tutorial e achar que está tudo certo. Então acho que é bom pensar na ferramenta que você tem mais confiança, que você tem mais conhecimento. Então, seguindo a ideia do Nicolás e do Daniel.

E já falando também, Daniel, vocês estão convidados aí para fazer outra live aqui com a gente, para ajudar aí o pessoal a colocar um DNS Recursivo aí em produção, tá? Já fica o nosso convite.

Bom, mas voltando para as perguntas, aqui tem do Leonardo Jorge dos Santos. Pensando em uma solução robusta, é possível ter um servidor DNS autoritativo, recursivo, Hyperlocal, com DNSSEC, DNS over TLS, DNS over HTTPS, então já pensando em tudo aí, se dá para fazer essas configurações dentro aí de um provedor. E se vale a pena ter tudo isso. Então, gostaria, Daniel, que você comentasse. E acho que uma das coisas também que dá para a gente falar de ter um DNS Recursivo, que você consegue talvez ali ter maior controle sobre os conteúdos que estão sendo providos aí no seu provedor, né? Que a gente já comentou isso em outras lives, sobre o DNS over HTTPS, que não dá às vezes para você fazer um controle parental, porque aí você está deixando a decisão para um terceiro. Então isso acaba dificultando. Então aí você tem ferramentas de DNS Recursivo, você consegue tomar algumas atitudes a mais. Manda bala, Daniel.

SR. DANIEL FINK: Tá legal. Bastante coisa nesse superservidor aí. Bom, primeiro, servidor de DNS autoritativo e servidor de DNS Recursivo deveriam estar separados. Deveriam ser máquinas separadas. Não no mesmo... não na mesma plataforma. São serviços diferentes que possuem vulnerabilidades diferentes. Então é meio que colocar todos os ovos na mesma cesta, tá? Então separe. Separem, deixa uma máquina só para o Recursivo, deixa uma máquina só para o autoritativo.

DNS sobre TLS ou sobre HTTP são assuntos bem novos, tá? São assuntos bem novos. Devem ser testados, podem ver como é que funciona. Então, acho que como o Eduardo falou, DNS sobre TLS é mais favorável para o provedor. O DNS sobre HTTP vai ser uma coisa mais para o lado da aplicação. Mas são assuntos novos. Eu diria que, por enquanto, usem isso em laboratório, tá?

Hyperlocal manda bala. A recomendação da Icann é: podem utilizar. Ele vai evoluir um pouco, a gente vai melhorar um pouco a forma de transferência de zona. Vai colocar um pouco mais de robustez nela, tá? Mas podem utilizar à vontade, inclusive em produção.

DNSSEC sim, por favor! Não deixem de fazer isso. Habilitem DNSSEC, essa é a nossa recomendação mais forte. Hoje em dia, do jeito que a internet está, a gente precisa ter DNSSEC funcionando em todos os recursivos. Beleza? E autoritativos também. Desculpa.

SRA. ANDREA ERINA KOMO: Bem, então o tempo está curto, já vou passar aqui para a próxima pergunta. O Anderson mandou para gente aqui, mais específico para o Nicolás: "Quando passamos a utilizar o DNSSEC, o mesmo propaga a sua chave pública para os demais servidores que utilizam o mesmo recurso?"

Então, Nicolás, por favor.

SR. NICOLÁS ANTONIELLO: Anderson, obrigado pela pergunta. Você tem que lembrar que se você está falando de assinaturas... Isso é para servidor autoritativo. Se você é autoritativo para um domínio, para uma zona, você tem que assinar. Sim? Pra usar o DNSSEC, você tem que assinar os seus recursos nesse servidor autoritativo. Se você está falando de servidor recursivo - que esta prática é sobre servidor recursivo -, você vai habilitar DNSSEC e seu servidor recursivo vai receber do servidor autoritativo todo o necessário para validar DNSSEC. Para saber se o recurso que você está consultando, se você, por exemplo, está consultando o registro A de um determinado endereço, de uma determinada... domínio, por exemplo, você vai receber o endereço associado a esse domínio, esse registro A, você vai receber a chave pública associado a esse recurso. E você vai receber também a firma digital desse recurso. A firma digital é basicamente... autoritativo cripta com a sua chave privada o Hash desse recurso. Você vai receber três coisas, basicamente: assinatura desse recurso, o recurso, e você vai receber também a chave pública. E, com isso, vai fazer a avaliação. E sempre vai receber isso do autoritativo. Acho que isso responde a pergunta.

E se quiser comentar algo mais sobre uma coisa que estavam falando previamente... se vai ocorrer no chat do Youtube comentou algo, mencionou algo que é muito importante. O que você nunca deve fazer é configurar e deixar para lá. Não tocar mais no servidor. Se você vai configurar um servidor autoritativo, recursivo, se você vai configurar... seja lá o que você for configurar, você tem que manter isso. Porque há fixes, patches de segurança que vão surgindo em tempo, e você tem que aplicar esses fixes, você tem que aplicar esse patches em seu servidor. Se você configura uma vez e nunca mais toca é provável que você receba um, dois, três milhões de ataques, e, finalmente, seu servidor provavelmente não sirva para nada. Então é muito importante sempre manter atualizado e administrar corretamente seu servidor.

SR. EDUARDO BARASAL MORALES: Muito bem colocado aí, Nicolás.

Bom, agora eu vou fazer uma pergunta minha para o Daniel Fink aí, porque a gente fez um hangout no passado aí sobre a troca de chaves do DNSSEC. Foi o roll over, né, e aí a gente tinha até comentado que isso daí deveria acontecer outras vezes no futuro. E aí, tem alguma previsão da Icann sobre isso, sobre esse assunto? Da troca de chaves do DNSSEC?

SR. DANIEL FINK: Legal, Eduardo. Nós tivemos a troca, a primeira troca da chave pública do DNS, a chave de configuração de chaves, a KSK, em 2018, tá? Dois anos atrás. A primeira foi instalada quando o DNSSEC foi implementado na raiz do DNS, em 2010. Então levou oito anos para uma troca acontecer, tá? E a gente tentou fazer toda aquela divulgação para o pessoal ficar esperto e verificar se o seu recursivo pegou a nova chave, tá?

Existem conversas na Icann para diminuir um pouco o tempo para uma nova chave. Talvez isso aconteça daqui a dois, três, quatro, cinco anos, não sabemos, tá? Mas, talvez, ela seja mais rápida do que a primeira troca, que aconteceu em 2018, levou oito anos para trocar. Então a gente vai prestar atenção nisso e vai informar para vocês. Por enquanto, sem previsão. E é isso, não vai ser no curto prazo. Beleza?

SR. EDUARDO BARASAL MORALES: Tá. Bom saber disso aí para não assustar ninguém aí com o DNSSEC, né?

Então, primeiramente, quero agradecer o Nicolás, agradecer o Daniel Fink por essa participação, por todos os comentários que vocês fizeram ao vivo, pelo vídeo gravado. Realmente foi muito esclarecedor tudo o que vocês mostraram aí para o pessoal, né? Então já deixo aqui os nossos agradecimentos. Também fazer agradecimentos aí à equipe de comunicação, todo mundo aqui que trabalha no backstage aí ajudando, então o Pedro, a Carina, a Drica, que estão aí nos ajudando. E a equipe dos cursos, que permitiu aí a gente conseguir fazer essa live aí de maneira fluida, que está ajudando aqui com as perguntas, a Tuane, a Erina, que está ajudando, o Moreiras, o Tiago e a Fernanda. Então deixo aí já nossos agradecimentos.

Vou falar uma coisa: pra amanhã, pessoal, também tem que fazer uma instalação prévia. Então a gente vai ter o laboratório lá do Luiz Puppin e do Lacier, que vão falar amanhã. E vocês têm que entrar lá no site da Semana de Capacitação, já baixar as máquinas virtuais, já fazer a instalação e já deixar preparado para acompanhar a live amanhã. Então não se esqueçam disso. Já faz a instalação prévia.

A gente já se encontra amanhã no mesmo horário, às 9h. Então a gente vai ter ali mais um dia da Semana de Capacitação. Então, um tutorial aí totalmente diferente para vocês aprenderem um pouquinho mais sobre redes, né? Colocando a mão na massa, né? Esses daí são diferentes das outras lives que a gente faz lá no Intra Rede, que é mais discussão. Aqui a gente está mostrando a configuração e está mostrando como trabalhar. Então a gente se vê amanhã.

E só o último aviso: quer o certificado dessa live? Até as 2h da tarde. E quem quiser nos ajudar colocando aí o seu comentário no formulário de avaliação, a gente vai botar aí o QR Code novamente. Então diz aí para a gente o que você achou dessa live, o que a gente pode melhorar. Se vocês querem a continuação dessa live, né? Já fazendo aí convite para o Daniel, para o Nicolás. Vocês querem ver como que coloca em produção certinho ali, passo a passo, aí a gente faz uma live de 8 horas aí, suga aí todo o conhecimento que eles têm para passar. Então--

SR. DANIEL FINK: A gente pode fazer uma live de música sertaneja?

SR. EDUARDO BARASAL MORALES: É, está aí de dupla sertaneja, os dois aí de chapéu, né?

[risos]

SR. EDUARDO BARASAL MORALES: Então, finalizar agora, pessoal, amanhã às 9h mais um dia da Semana de Capacitação. Muito obrigado e até mais!

SR. NICOLÁS ANTONIELLO: Tchau, tchau!