SR. EDUARDO BARASAL MORALES: [interrupção no áudio].

ORADOR NÃO IDENTIFICADO: Eduardo, você está no mudo.

SR. EDUARDO BARASAL MORALES: Opa! Desculpa, pessoal, eu estava no *mute* e estava falando aqui com vocês. Então, bom dia a todos. Sejam bem-vindos aí ao quarto dia da nossa Semana de Capacitação, que a gente teve aí tutoriais técnicos, como aí de instrumentação óptica, FTTH, a gente teve, também, de *communities,* e agora a gente vai ter sobre segurança, que convidamos o pessoal do CERT.br. Então, a gente está muito feliz com essa semana, todos vocês participando muito, mandando perguntas no chat. Está sendo muito proveitoso.

E antes da gente ir para os nossos palestrantes, eu gostaria de agradecer aos nossos patrocinadores, que é a Juni Link IP e Cloud Network by Giovaneli Consultoria, WZTECH Networks, ICANN, Netfinders Brasil, Novatec Editora, Solintel, Cisco e Logicalis, 4Bios IT Academy, Globo, Netflix, Fiber X, Huawei e o apoio de mídia da revista RTI e Infra News Telecom, tá?

Eu gostaria de lembrar que essa live vai ter certificado. Então, quem quiser, precisa se inscrever no link que está sendo colocado agora no chat do YouTube, vai ficar disponível até às 14h e vai ser enviado um e-mail, e nesse e-mail vai ter um link ali de confirmação. Clicando no link de confirmação, depois você vai receber ali o certificado.

Lembrando a vocês que a gente tem um projeto aí chamado Cidadão na Rede, que a gente visa ensinar um usuário comum a ser um bom cidadão na Internet e como escrever ali uma boa senha, não é, para ter ali uma segurança básica, não é, como não repetir senhas... Eu estou falando aí os de segurança, mas a gente tem várias coisas relacionadas à infraestrutura, padrões Web, tá, direitos e deveres, que é muito interessante. E eu gostaria de pedir a ajuda de vocês para divulgar esses vídeos, e aqueles que são empresas, que assinem o projeto, não é? Se cadastre, coloque o logo dentro ali do videozinho, pegue aquele videozinho e mostre para os seus clientes, mostre para os seus funcionários, divulguem essa ideia, porque se a gente melhorar a Internet no usuário, mesmo nessa questão de segurança, melhora a Internet para todos. Então, ali é uma questão de a gente ter a consciência social na Internet, não é?

Bom, não vou me alongar mais, pode tocar aí o videozinho do Cidadão na Rede.

[exibição de vídeo]

SR. ANTONIO MARCOS MOREIRAS: A Cristine e o Klaus, que estão aqui com a gente hoje, são grandes colaboradores dessa série de vídeos aí do Cidadão na Rede, não é? Toda a equipe, toda a equipe do CERT tem nos ajudado muito com temas, com ideias para esses vídeos aí, porque um dos temas que a gente trata nessa série de vídeos é justamente temas relacionados à segurança, segurança da Internet. Esse, por exemplo, aí de hoje, de que... Na verdade, hoje, o celular da gente, é... ele tem a importância de uma carteira, não é? Se você perder o celular é a mesma coisa de você perder a carteira, está cheio de documentos lá, tem acesso a banco, tem um monte de coisa. Bom, gente, fica aí o convite para vocês darem uma boa olhada no site Cidadão na Rede, nesses vídeos.

E bom dia a todos e todas. Sejam muito bem-vindos aqui novamente à Semana de Capacitação do NIC.br, organizada aqui por nós do Ceptro. Hoje, o nosso tema é Segurança Avançada para um Provedor, a gente vai ter o pessoal do CERT.br, e eles vão falar de *hardening*, *hardening* de equipamentos; de redução de ataques de DDoS, que eu tenho certeza que todo mundo aqui que é de provedor é um tema que vocês estão bastante atentos, que dá dor de cabeça em muita gente; como é que você pode usar o *netflow*, os *netflows*, não só para ver se o teu tráfego maior é o do Google, do Netflix, de sei lá mais quem, mas para identificar problemas de segurança; como receber e tratar aquelas notificações, não é, o que a gente faz com aquilo, às vezes, o pessoal dos provedores fica na dúvida; e muito mais. Então, o Klaus e a Cris vão estar aqui. Vai ser, também, diferente do primeiro e do segundo dia da Semana de Capacitação e um pouquinho diferente de ontem. Por quê? Porque o Klaus e a Cris vão estar interagindo com vocês ao vivo, não é? Então, eles não estão... A aula não foi pré-gravada. A aula de hoje não foi pré-gravada, a palestra de hoje não está pré-gravada, eles estão aqui interagindo ao vivo, só que eles combinaram com a gente que eles vão estar atentos ao chat do YouTube. Então, vocês podem ir fazendo as perguntas que eles vão estar lendo no chat do YouTube e vão estar respondendo ali na hora, não é, assim que for possível, não é, assim que der para encaixar ali no tema que eles estão tratando. Na hora é o jeito de falar, não é? O pessoal já ia fazer cara feia aqui para mim. Eles vão estar atentos, vão estar ali olhando as perguntas, na medida do possível, eles vão encaixar as respostas no meio das falas da apresentação deles ali, conforme a pertinência, tal. E a gente também, da nossa parte aqui, vai ajudar eles, anotando as perguntas também e, depois, mais para o final ali, colocando uma relação para eles.

Bom, gente, estamos aqui com 337 pessoas assistindo agora, 339, está subindo aqui. Só 112 *likes*, não é? É bastante pouco. É muito pouco ainda. Então, eu peço para vocês, primeiro, deem os *likes*, não é? Isso ajuda na distribuição do vídeo pelas plataformas, pelo YouTube,

pelo Facebook, na distribuição que a gente chama de distribuição orgânica, que é aquela distribuição que não depende de propaganda, e a gente se baseia nisso. Às vezes, mesmo a pessoa que está inscrita no canal do NIC.br, ela não recebe o aviso de que a live está rolando, de que o vídeo está lá disponível, não é? Agora, quando o vídeo tem mais *likes*, a plataforma tende a distribuir, a mostrar que aquele vídeo está disponível para mais gente. Então, o *like* de vocês pode ajudar esse conteúdo que a gente sabe que vai ser um conteúdo muito bom, muito importante para o pessoal dos provedores. Tanto agora quanto depois, quando ele fica gravado aqui, esse conteúdo fica disponível para mais gente quando tem mais *likes*. Ele é achado, ele é encontrado por mais gente quando tem mais *likes*. Por isso que eu insisto bastante aqui, não é? Vocês sabem que o NIC.br é uma instituição sem fins de lucro, esse canal não é nem monetizado, a gente não está interessado em tráfego por ter tráfego, em gente assistindo por ter gente assistindo. A gente tem um conteúdo importante, recados importantes, boas práticas importantes para ensinar para vocês, para ensinar para o pessoal dos sistemas autônomos, para ensinar para os provedores, e o *like* de vocês ajuda muito a gente nisso daí, não é? Então, é importante, deixem o seu *like* no vídeo. E está na hora, também, vocês que têm aquele grupo do Facebook que vocês fazem parte, o grupo do WhatsApp, o grupo do Telegram com o pessoal dos provedores, com o pessoal aí do trabalho, com o pessoal que está interessado nesse tema de segurança, está na hora de vocês colocarem o link lá. Dá tempo ainda. Fala: "Ó, pessoal, começou a Semana de Capacitação aí hoje, na quinta-feira, e está naquela hora que o Moreiras fica lá só enrolando e pedindo *like*, para dar tempo de o pessoal acordar e entrar no vídeo". Então, deixem... coloquem lá o link para a gente encher a sala aqui, para quando eu passar a palavra para a Cristine e para o Klaus, não é, a sala estar cheia e ninguém perder nada. Mas se perder, também, depois, temos a gravação, vai ficar tudo aqui registrado, tudo gravado, e fica fácil também de o pessoal assistir depois.

E eu estou vendo aqui que tem gente que está querendo o moletom do IX.br, não é? Tem gente pedindo o moletom do IX.br aqui no chat. Eu vim de propósito com ele, porque já pediram ontem. Eu, de novo, coloquei ele, e não foi por acaso, não. É bonito também, não é? Eu acho bonito para caramba. Então, gente, vocês podem ganhar, sim, o moletom do IX.br. É assim, as regrinhas para ganhar o moletom do IX.br estão em um site chamado nic.br/vagas, e tem lá vagas em aberto para o IX.br, relacionadas ao IX.br. Então, se você... se acharem que vocês se encaixam naquelas vagas, vocês preenchem um formulário chamado Currículo e mandam lá para o e-mail selecao@nic.br. E, se vocês forem selecionados, então, vocês podem, no final do processo, também ganhar um moletom do IX.br. O que vocês acham? Eu acho interessante, nic.br/vagas.

Pessoal, digam aí para a gente no chat... Já vou passar a palavra para a Cristine e para o Klaus. Digam para a gente no chat se é o primeiro dia de vocês aqui na Semana de Capacitação ou se vocês já acompanharam na segunda, na terça e na quarta-feira. Eu estou interessado... a gente está interessado em saber quem está aqui pela primeira vez e quem já está aqui durante a semana inteira. Olha aqui, tem bastante gente chegando aqui pela primeira vez, que a gente acabou fazendo temas um pouco diferentes. Nos dois primeiros dias, a gente tratou sobre tecnologias ópticas, fibras ópticas; ontem foi algo mais relacionado a roteamento; e hoje nós temos segurança. Então, todos os temas interessam ao pessoal técnico dos provedores, aos analistas, aos engenheiros, aos técnicos que trabalham nos provedores, mas, às vezes, tem as pessoas que são mais especializadas, não é? Quem cuida da parte óptica, às vezes, não está cuidando do roteamento, não está cuidando da segurança, ou simplesmente o pessoal, às vezes, não sabia da semana e chegou aqui só desavisado. Amanhã temos CDNs, temos o tema de CDNs, temos seis CDNs que vão estar aqui... representantes de seis CDNs aqui presentes com a gente falando sobre justamente como os provedores podem se conectar com elas de uma forma melhor. Bom, legal, bastante gente aqui. Ezequiel no quarto dia, Lucas de França no terceiro dia, Alberto no primeiro dia, Lourival no terceiro dia, Anchis no primeiro dia, João Paulo Nery no primeiro dia. O Eduardo Barasal Morales disse que está aqui no quarto dia já. Ainda bem, não é, Barasal?! André Yannatos no terceiro dia, Renato Madrid, primeiro dia, Emílio Arinnatos (sic), primeiro dia. Então, pessoal, vocês que estão vindo pela primeira vez, espero que vocês gostem. Deixem já seu *like* aqui para a gente, deem aquele voto de confiança. Se vocês não gostarem da aula da Cristine e do Klaus, no final, vocês voltam aí e tiram o *like*, não tem problema nenhum, vocês têm o direito de fazer isso. Dá o voto de confiança para a gente, porque o conteúdo vai ser bom. E já estamos, agora, com 440 pessoas on-line aqui.

Eu vou, então, passar a palavra para a Cristine e para o Klaus, que vão dar essa aula de segurança para a gente, e desejo boa aula a todos. A gente volta a se falar aí um pouquinho mais para a frente, durante a live. Até mais! Boa aula.

SRA. CRISTINE HOEPERS: Obrigada, Moreiras. Muito obrigada aí a todo mundo. Eu sou Cristine, não é? Eu estou aqui no CERT.br desde a época que nem chamava CERT.br, que era o NBSO, não é, e a gente está aqui tentando ajudar a segurança da Internet, como um todo, a crescer. E estou muito contente que tem bastante gente, estou vendo ali que a gente já passou de 400 nesse momento, e eu queria passar palavra para o Klaus, para ele dar um bom dia aí para vocês também.

SR. KLAUS STEDING-JESSEN: Pessoal, bom dia a todos. Meu nome é Klaus, é um prazer estar aí com vocês. Como o Moreiras falou, a gente vai tentar levantar vários assuntos relevantes no contexto de segurança de um provedor, tá, e vamos tentar, também, responder a maior quantidade de perguntas aí possível, tá? Então, bom dia a todos, e a gente já pode começar aí.

SRA. CRISTINE HOEPERS: Falando em começar, deixa eu só compartilhar os slides. Eu não sei... O Morales acabou não falando, mas os slides, a gente já deixou o PDF com eles, talvez já esteja até na página do evento, tá? A nossa ideia é que esses slides fiquem públicos aí para vocês poderem aproveitar alguns comandos, algumas coisas aí que a gente deixou nesses slides aí, tá?

Então, como o Klaus falou, a gente quer falar um pouco aqui de segurança de provedores, não é? Apesar de dizer ali "segurança avançada", o que a gente tentou trazer são, realmente, os problemas que a gente está vendo que estão afligindo mais, que estão gerando mais incidentes, que estão gerando mais problemas, não é? E a gente queria compartilhar isso tudo com vocês e talvez deixar claro que não tem nada, assim, tão complexo que precisaria ser feito. São coisas que dão trabalho, são coisas que vocês vão ter que se dedicar, tem um pouco de planejamento, mas que eu acho que iam reduzir muito os incidentes de maneira geral para vocês aí se vocês adotarem.

Essa semana... Eu vou falar... Antes de começar a falar das estatísticas e de coisas aí, para quem não conhece o CERT.br, não é, a gente está aqui trabalhando no Brasil desde 1997, não é? A gente foi criado a partir de um relatório aí do Comitê Gestor da Internet, da importância de ter alguém para tentar aumentar a segurança de redes no Brasil. A gente atende a qualquer rede que use algum recurso administrado pelo NIC, tá? Então, qualquer um que tenha um IP, uma AS ou um domínio aqui no Brasil a gente atende, a gente tenta ajudar nessa parte de incidentes, não é? Então, a gente tem uma parte-chave que é a de gestão de incidentes, que, provavelmente, todo mundo que está assistindo essa live aqui já recebeu alguma notificação nossa, principalmente quem é de provedor já deve ter recebido algum contato nosso aqui, não é? Então, essa é uma parte, eu acho, que vocês têm mais contato. A gente tem uma área, também, grande, de consciência situacional, que é uma área nossa onde a gente tem nossos *honeypots* e a gente compartilha informações, e também muita gente aqui recebe notificações nossas que são de ataques que a gente vê saindo das redes de vocês e chegando nos nossos *honeypots*, a gente também trata com alguns *threat feeds*, não é? A gente tem parceria com Shadowserver, com Team Cymru, com Shodan; recebe, algumas vezes, aqueles dados de ações *anti-botnet*, e aí a gente entra em contato com todos os ASs também para avisar dos problemas, não é? E a gente tem uma área grande de conscientização e treinamento, não

é? A gente tem o desenvolvimento de materiais para administradores de sistemas, que hoje estão lá no site do bcp.nic.br, no nosso site. A gente tem muita coisa para o usuário final, não é? Tem a cartilha de segurança, tem os materiais para crianças, que estão lá no portal internetsegura.br, e a gente tem também os cursos da área de tratamento de incidentes e um trabalho aqui com a equipe do Moreiras aí de ajudar eles lá no Cidadão na Rede, dando palpites, de também participar aqui dessas Semanas de Capacitação, mas sempre com o objetivo de trazer para a comunidade o que a gente está aprendendo nessas duas áreas aqui, não é, quer dizer, o que a gente está vendo no incidentes e o que a gente está vendo acontecendo na Internet aí de maneira geral, não é?

Então, falando um pouco aí dessa parte de provedores, não é, foi muito interessante, a gente estava aí chegando perto de dar esse tutorial, e essa semana, o começo da semana, a gente começou a ter umas notícias aqui, não é, e a gente já tinha uma sessão grande dos ataques mais prevalentes, e a gente começar a discutir onde estão, realmente, os problemas, não é, para daí a gente pensar o que fazer para melhorar a segurança. E aí, essa semana a gente teve um *press release* de uma empresa que mostrou lá: "Olha só, tivemos 13 bilhões de tentativas de ataque, e o Brasil lidera o *ranking*", e é claro, não é, você tem... para alguém ler as matérias, você precisa ter as... os títulos são quase *clickbaits*, não é, só que eu comecei a refletir, e eu e o Klaus, a gente conversou um pouco, não é? Quer dizer, "*hackers* elegem o Brasil como alvo", não é? Será que *hackers* elegem alguém como alvo hoje em dia, não é? Quer dizer, como funciona esse negócio de ataques, não é? É isso mesmo? E o outro era: "Metade dos ataques da América Latina foram contra o Brasil". Isso é muito ou isso é pouco? Não é? Não sei se o Klaus tem alguma resolução--

SR. KLAUS STEDING-JESSEN: E outra coisa--

SRA. CRISTINE HOEPERS: É.

SR. KLAUS STEDING-JESSEN: Outra coisa para a gente refletir também, não é, Cris, sempre que a gente vê essas matérias, como você chamou, meio "*clickbaits*" aí, o que é exatamente 3,2 bilhões de tentativas, não é? São entradas de linhas de *Log*, são tentativas... não é? Então, assim, esse é outro número que, às vezes, a gente fica meio com o pé atrás, não é? Então, assim, só para a gente ter um pouco de senso crítico, acho, quando a gente vê notícias por aí, não é? Bem como você falou, é muito? É pouco? E o que é 3,2 bilhões de tentativas, não é?

SRA. CRISTINE HOEPERS: Exato. E aí, eu ainda acho, assim, não é, "*hackers* elegem o Brasil"... Bom, as ferramentas automáticas gerando ataques estão varrendo a Internet dia e noite, não é, e vão achar e vão atacar uma Internet de um tamanho grande, não é? E aí,

antes de a gente falar, não é, lembrar sempre, pessoal, daquelas estatísticas básicas, não é? A Internet brasileira é grande na América Latina, não é? A gente tem 62% dos IPv4s e 71% dos sistemas autônomos. Então, eu estranharia, e eu gostaria de chegar, na verdade, em um ponto em que dissesse assim: "Olha só, só 10% dos ataques eram no Brasil", quer dizer, que a gente estaria muito melhor do que a média. E o que se esperaria é assim: se você tem alguém com sensores e *firewalls*, IDSs, não é, que é o que a empresa lá vende, pegando *Logs* de ataques chegando nas redes, você vai ter mais coisas no Brasil, porque a nossa rede é muito maior. Então, antes da gente começar a falar de incidentes, de mais dados, e sempre a gente refletir que tudo tem um contexto, não é, o contexto do tamanho da nossa rede, o contexto do que a gente tem de equipamentos e exposto aí, lembrar que toda rede que é maior vai aparecer mais nas estatísticas de ataques, não é? Então, a gente tem sempre que levar isso em conta, e a gente quis fazer um pouquinho essa reflexão antes de entrar aí em estatísticas mesmo, não é?

Mas aí, a gente pensando, não é, o que são os ataques mais comuns e como que as coisas mais acontecem, não é? Tem várias estatísticas, mas eu tentei pegar aqui alguns relatórios, assim, mais específicos de quem está acompanhando as causas dos incidentes, não é, e tem um relatório muito interessante de uma empresa que... eles fazem só *pentest*, não é, e aí eles fizeram uma estatística dos *pentests* contra empresas. Até aí já estamos pensando assim: essa empresa... eles são contratados por empresas que estão querendo testar a segurança que já foi implantada. Então, até se imagina que são ataques contra empresas que têm a segurança um pouco acima da média, não é? E aí, a gente começa a olhar: 77% dos... de como eles conseguiram entrar nessas redes, nessas empresas, foi com esses ataques aqui, que, se vocês olharem, de baixo para cima é: uma força bruta de credenciais de FTP; força bruta de credenciais de domínios compartilhados ali junto com alguma vulnerabilidade; força bruta de credencial de acesso remoto; força bruta de credencial de acesso de banco de dados. Aí... Ah, aplicações Web, mas dentre as aplicações Web, a primeira, qual é? Força bruta de credenciais, não é? E aí, vulnerabilidades em software, mas olhem que a minoria são os *zero-days*, quer dizer, as vulnerabilidades não conhecidas, não é? Então, eu acho que, assim, a gente estaria muito melhor se o pessoal fizesse o básico, não é, que é *patches*, senhas e ter políticas, não é, inclusive de senhas, não é?

Aí, se a gente for pensar um pouco mais para frente, tinha uma outra matéria muito interessante do pessoal falando que: "Olha, hoje em dia, todo mundo acha que os ataques são supersofisticados". Não, não, eles voltaram para o mais básico. O que a gente vê funcionando hoje em dia é o que funcionava no início dos anos 90: são senhas

fracas, senhas furtadas, de alguma maneira comprometidas, não é? Acho que esse foi o ano que... a gente está vendo aí muitos vazamentos de dados, e o que mais aparece, quase que semana sim, semana não, é alguma base de dados de senhas vazadas e que apareceram por aí na Internet. A gente até vai ver um pouco como isso está afetando incidentes grandes de senhas que vazam por aí.

Uma outra coisa é a gente pensar o que é *patches*, não é? A gente imaginaria que se você tem empresas que têm uma VPN, e a VPN, ela é o ponto de entrada na sua organização, que é por onde as pessoas vão conectar, esse seria o servidor mais seguro que você teria, não é? E aí, a gente pensa que a gente teve 900 organizações comprometidas por causa de uma vulnerabilidade em um software de VPN, que era esse Pulse Secure VPN, por quê? Porque era um CVE com mais de um ano, era uma vulnerabilidade velha, e que daí tem aquela visão: "Ah, mas ninguém está explorando". É, ninguém está explorando até o dia que alguém explora, não é? E aí, você tem 900 organizações que, em uma tacada só, foram comprometidas, não é? Então, assim, a lição é: se você tem algo que está mapeado como crítico, que está de frente para a Internet, não pode deixar para amanhã instalar *patches*, não é? Os *patches* têm que ser instalados assim que sai uma vulnerabilidade. Então, isso eu acho que é uma coisa que a gente vê acontecendo de novo, e de novo, e de novo, não é, essa coisa do: "Ah, mas tem alguém explorando?". Eu falei: Um, você não sabe, não é, pode ter, sim, alguém já explorando, mas o outro é que na hora que alguém faz uma prova de conceito, ela quase que imediatamente já vira um *malware* e você tem aí todo mundo explorando essas vulnerabilidades aí.

E eu acho que, assim, nessa linha de coisas básicas que levam a grandes acidentes aí, não é, desse ano, eu acho que foi o ano de vazamento de dados, e *ransomware* realmente subiu muito, não é, mas é a gente pensar ali, pessoal, que, assim, todo aquele incidente da Colonial Pipeline, que parou a distribuição de combustível em toda a costa leste americana, era uma senha que tinha sido vazada na *dark web.* Quer dizer, eles tiveram uma senha comprometida em uma conta de VPN, que, provavelmente, quem usava aquela VPN teve o seu *desktop* ou *notebook* comprometido. O que é mais duro ainda é que era uma conta antiga e que já nem era mais usada, mas que ficou abandonada lá, então você tem os problemas de não fazer gestão de configuração, de não limpar conta quando o funcionário sai da empresa. Reuso de senha é algo normal, ter uma VPN só com senha é um problema, não é, e isso daqui ficou público, não é? Foi um relatório feito, você teve até o CEO da Colonial Pipeline, ele foi no Senado americano e falou isso, ele falou: "Não, não era uma senha simples, não foi chute de senha, era uma senha complexa". Mas aí era só senha, não é, era só senha.

Klaus, você está acompanhando? Tem alguma pergunta relacionada com isso aqui? Você quer fazer algum comentário? Que eu, enquanto estou falando, eu não estou conseguindo ver o chat.

SR. KLAUS STEDING-JESSEN: É, na verdade, eu queria fazer um comentário, Cris, que a gente... Vocês viram, não é, pessoal, que a gente tirou aquele "segurança avançada", não é? Justamente para remeter até a essa introdução que a Cris está dando, que é justamente isso daí: você não precisa, como aquele artigo botou lá, o *space-age technology*, não é? Você não precisa ter um negócio mirabolante, tá? Muita gente pensa: "Cara, vou ter que despender milhões aqui, vou ter que ter um monte de *appliances* de segurança", não é, quando, na verdade, o que a gente está querendo mostrar aqui é que assim, é usar Pareto aqui, pessoal, tá? Vinte por cento de esforço de vocês vai pegar 80% desses casos aí de comprometimento. Estamos falando de grandes, tá, Colonial Pipeline, e nós estamos falando de quê? Senha, ou seja, não tinham múltiplos fatores de autenticação; estamos falando de *patches* de coisas antigas, tá? Então, não é o *zero-day*... Então, isso, eu acho que, assim, seria a mensagem até aqui, tá, que a gente queria muito que... passar, tá? Só reforçando isso aí, Cris.

SRA. CRISTINE HOEPERS: Sim. Eu até dei, agora uma escapadinha, olhar o chat, não é, daí o pessoal: "Ah, os ataques evoluíram e as empresas pararam no tempo". É o contrário, não é? As empresas pararam no tempo, sim, e os atacantes não precisam evoluir, tá? Essa que eu acho que é a tristeza e o comentário aqui com esse comentário do Klaus. Quer dizer, assim, a gente tem aqui na nossa sala um pôster do OpenBSD na época em que eles fizeram o OpenSSH, que era assim: "*Rest in peace*", não é, o RSH, Telnet, tal, não sei o quê. Infelizmente, não foi *rest in peace*, não é, porque as pessoas continuam usando Telnet, continuam não usando chaves criptográficas, cuidando não cuidando de senhas, e hoje a gente está tendo até um ponto que está muito complicado. A gente não botou nenhum caso aqui, mas se vocês fizerem aí umas buscas, vocês vão ver que tem alguns relatórios de um pessoal que está fazendo acompanhando de GitHub, tá, e um lugar que está tendo vazamento de senha direto são desenvolvedores que põem uma senha *hardcoding* no código, sobem no GitHub, e o pessoal está pegando chaves de *[ininteligível]*, está pegando todas aquelas credenciais criptográficas de *buckets* de *cloud*, está pegando senhas internas, tudo via código-fonte no GitHub. Então, assim, hoje a gente está tendo múltiplas maneiras de vazamento de senha, e aí o problema vai, de novo, em usar só senha como--

SR. KLAUS STEDING-JESSEN: Cris, o pessoal está brincando no chat aqui, um exemplo de Cisco123, mas assim, a gente já viu muita senha "alguma coisa 123", não é? Isso aí--

SRA. CRISTINE HOEPERS: Sim.

SR. KLAUS STEDING-JESSEN: Sim, isso acontece na prática.

SRA. CRISTINE HOEPERS: E a gente vai falar disso até um pouco mais à frente, em incidentes bem sérios aqui no Brasil que era isso aí, tá?

Só que aí vamos falar de vulnerabilidades. "Ah, meu Deus", não é, "mas a gente tem governos atacando", não é? É muito interessante que já no passado o pessoal do CISA lá, que é o novo nome do US-CERT, eles divulgaram, de 2016 a 2019, quais foram as vulnerabilidades mais exploradas por atores de alto valor, quer dizer, por outros governos e tentando comprometer redes de alto valor americanas. Vocês pensem que... É 2016 a 2019, não é? Os mais usados são de 2012, 2015, 2017, 2018, não é? Então, assim, você esperaria que a gente teria... não teria coisas de 2012 sendo exploradas por um *cyber [ininteligível]* essas coisas aí que você fala: "Não, mas o governo da Coreia do Norte está fazendo", "porque o governo da Rússia teria a capacidade". O que eles têm é um bom indexador de *exploit*, CVEs, estão lá usando. Por quê? Porque isso está sem aplicar *patches*, não é? Hoje em dia, muito problema com Office 365, não é? A gente está vendo muito *Phishing* de Office, porque todo mundo moveu, e aí você conseguindo essa conta, você acaba conseguindo acesso a e-mail, acesso a documentos importantes, não é? Então, assim, não precisaria nem ter a parte de *exploits*, não é, você poderia só ter a parte de *Phishing* envolvendo tudo isso aqui. Lembrando que *Phishing* de Office 365 teve, sim, um papel naqueles incidentes da SolarWinds do ano passado, que foram atribuídos ao governo da Rússia, não é? Então, muito relatório público aí falando disso também.

Um outro ponto que a gente queria mover um pouco mais para ameaças de rede, não é... Tem um relatório muito interessante que o pessoal da Rapid7, não é, que é o pessoal que mantém o Metasploit, mantém outras ferramentas, faz, que eles têm uma rede de *honeypots* e eles ficam varrendo o espaço, o endereçamento IPv4 à busca de vulnerabilidades e o que está exposto na Internet. Não tenho o de 2021 ainda, esse aqui é o de 2020, é o mais atual que eles têm. E se a gente for olhar o que eles têm ali... Quer dizer, quem são os países que estão mais expostos? Sim, a gente imaginaria que o Brasil está exposto, não é? Por quê? Porque a gente tem uma das maiores redes, a gente tem muito IP, a gente é uma rede grande, não é, mas se a gente for pensar, tem outras redes, também, muito grandes que estão atrás, tem redes não tão grandes como a nossa que estão na frente, então é meio variado, não é? Mas o que é isso? São: um, você, sim... quem tem mais IPv4 exposto tem mais coisas para atacar, mas tem serviços que eles até põem aqui, olha: "Isso nunca deveria estar exposto", que são

todos aqueles serviços como Telnet, SMB, SQL Server, RDP. Essas coisas não deveriam estar de cara para a Internet na maioria das vezes, não é? Então, como é que está o Brasil, onde que a gente está mais exposto?

Bom, Telnet, tá? Isso é uma coisa que a gente continua vendo, vocês vão ver que a gente vai falar dos nossos ataques, não é, e aí a gente vê... Assim, quem está mais exposto? O que eu estranho nesse gráfico é ver a Argentina tão mais alto que o Brasil, não é, mas a gente sabe que lá também tem equipamentos, não é, e provavelmente tem muito CPE, muito modem de banda larga que está exposto, não é? A gente tem a China muito exposta, Brasil. Mas aqui, quem são os *vendors* mais expostos? Cisco, Huawei, Mikrotik, não é? Isso aqui tem... já começa, principalmente para quem é provedor de acessos, você começa a ver que é, sim, muito da infraestrutura *core* de banda larga que está aí aberta com Telnet. IoT também está aí aberto com Telnet. Mas quando você olha isso daqui e vê que isso daqui são equipamentos de rede, não é, por mais que a gente tenha, também, CPEs, Mikrotik, Huawei e tal, não é IoT, não é termômetro conectado na Internet, não é... não é? A gente está falando mais aqui de coisas que afetam o pessoal de provimento de acesso.

Klaus, eu vou tocando, quando você quiser parar e interromper, você vai interrompendo, porque senão eu vou indo, tá?

SR. KLAUS STEDING-JESSEN: Não, não, vai, sim, vai, sim. Tinha um comentário ali, Cris, se o pessoal já tinha ouvido falar do Shadowserver Foundation. Talvez, se você quisesse só relembrar lá que uma das nossas fontes de dados lá naquele primeiro slide, um dos primeiros slides que você mostrou, de *threat feeds*, é do Shadowserver, não é? Depois, a gente pode, quem sabe, voltar nesse assunto, quando falar--

SRA. CRISTINE HOEPERS: Nesse assunto.

SR. KLAUS STEDING-JESSEN: De amplificação, etc., não é?

SRA. CRISTINE HOEPERS: Não, com certeza. Inclusive, lá na amplificação, tem um link para o Shadowserver, para o site deles, aí a gente coloca lá.

Bom, o que é o segundo serviço que a gente tem ali? SMB 445. A maioria é Windows, mas sim, tem muito samba aqui, muita coisa em Linux, não é? O Brasil é um dos top países aqui, não é, e pensar toda a questão ali de... que WannaCry era isso aqui, não é, era SMB, tá? Então, é lembrar que tem muita coisa sendo explorada nessa área aí.

Outra coisa... Assim, eu vi um pessoal comentando no chat ali, falando: Ah, na pandemia ficou mais exposto, tal, não sei o quê. Sim, realmente, embora esses dados aqui são até um pouco antes de pandemia. Já tinha muito RDP exposto na Internet, e sim, a gente está

também exposto, e tanto SMB quanto o RDP tiveram grandes vulnerabilidades nesse período aí. Então, a gente tem não só força bruta de credencial, mas a gente tem, também, vulnerabilidades sérias, não é, que ficaram expostas com esses dois serviços aí na Internet.

E se a gente for mover agora, para tentar ver um pouco de Brasil, não é, os nossos dados aqui do CERT.br, dos nossos *honeypots*, não é... Então, a gente tem uma rede de *honeypots* que tem sensores em vários parceiros no Brasil. Na página ali que está no link desse slide tem link*s* para todos os parceiros, para onde está. A gente mantém dados diários disponíveis lá do que está sendo visto nesses *honeypots* desde 2017, se eu não me engano, a gente tem esse diário, os *flows*, tá? E o que a gente está vendo--

SR. KLAUS STEDING-JESSEN: Cris, e só um parêntese.

SRA. CRISTINE HOEPERS: Oi?

SR. KLAUS STEDING-JESSEN: Veio em boa hora os dados aí dos *honeypots*, tem justamente uma pergunta perguntando sobre o projeto aí dos *honeypots* e qual é o maior vetor de ataque atualmente no Brasil. Essa é a pergunta exatamente, tá? Então, talvez, para a gente mostrar que, olha, não difere muito isso que a gente está vendo nos top portas varridas do relatório que a Cris acabou de mostrar, tá? Assim, isso é uma tendência global, não é?

SRA. CRISTINE HOEPERS: Exato. E o que eu acho... Assim, o que a gente vê nos nossos *honeypots*? É o que o mundo está procurando nas nossas redes, não é? E se o mundo... Aqui vale também um pouco a lei de oferta e demanda, não é, e se a gente for pensar, a gente está com isso aí exposto na Internet, é o que o pessoal está procurando para atacar. E aí, a gente vai ver aqui coisas que a gente não vê no Rapid7 com mais detalhes, mas lá já tinha Mikrotik, só que a gente está vendo aqui não é só Telnet, Mikrotik, a gente está vendo aqui também o Winbox e a API. O pessoal está direto atacando, não é, e a gente vê comprometimentos de incidentes que a gente lida que são em cima disso aqui, tá, em cima de Mikrotik. Vocês podem ver que Telnet é 94% das tentativas que a gente pega, mas a gente tem muitos *listeners*, não é, a gente emula Telnet, então, nesse caso, a gente também... em termos de volume de dados, a gente coleta mais mesmo, não é? Se a gente for pensar, é o quê? É Telnet, 445, SSH, sim, força bruta de senhas em qualquer coisa que tenha senhas, RDP Web, procurando N coisas com protocolos aí, e Web exposto. A gente tem, ainda, muita coisa em IoT, que também usa http, e não usa https ainda, não é, mas todo mundo está procurando https também; FTP, Microsoft SQL. Então, assim, se vocês forem olhar, no fundo, é muita vulnerabilidade e força bruta de senha. É isso que eles estão procurando, não é? E a gente tem os nossos emuladores aqui, o que o

pessoal está tentando é força bruta de senha. Por exemplo, em Web, uma das coisas que a gente vê bastante em Web, é o quê? Força bruta de senhas de Wordpress, de senhas de [ininteligível] de senhas de administração de ICMS, de sistema de conteúdo. Então, assim, mesmo o Web, o pessoal está procurando o quê? Força bruta, porque é o que a gente vê que está funcionando, não é? Então, no fundo a gente mostrou muito esse cenário global, porque a gente queria ver... do tipo: "Olha, a gente está vendo algo muito diferente do cenário global?". Não, a gente está vendo mais ou menos isso aí, tá? É o que a gente também está vendo nos *honeypots*.

SR. KLAUS STEDING-JESSEN: E mais um comentário de http, Cris. Isso também, às vezes, é usado para mexer em configuração de CPEs, não é? Muitas vezes, CPEs têm porta 80 habilitada sem autenticação, permitindo mudar algumas configurações de maneira remota. Isso a gente tem visto nos *honeypots* também, não é, mudança de servidor DNS, por exemplo, que a gente vai falar um pouquinho mais para frente.

Outra coisa aqui, pessoal, são esses serviços expostos de Windows, tá? Não é bem o nosso tópico aqui, a gente vai falar mais de provedores, mas, por exemplo, todo mundo hoje em dia, com a pandemia, que está trabalhando de maneira remota, não é, está trabalhando em casa, é algo para se perguntar também: Como que é está esse ambiente em casa, não é? Tem um Windows de frente para a Internet que está sendo explorado, muitas vezes a pessoa que está lá em casa não tem, necessariamente, um perfil técnico, não é, não tem a mínima ideia do que está acontecendo, e enquanto ela trabalha no dia a dia, a máquina dela está sendo lá... Por exemplo, principalmente essa parte de RDP, não é? Então, acho que outro ponto de atenção aí, não é?

SRA. CRISTINE HOEPERS: Exato. E aí, eu estava agora dando uma olhada, não é, o pessoal perguntando sobre ataques em IPv6, não é? A gente vê coisas em IPv6. É bom lembrar que IPv6 ainda não tem muito *malware*, porque, realmente, o *modus operandi* dos atacantes é, geralmente, varrer a Internet inteira. Aí, sim, não escala, fica varrendo o espaço IPv6, não é? E aí, tem aquela outra questão: Está funcionando atacar IPv4? O pessoal não está movendo muito, mas todos esses ataques que a gente falou até agora independe se é IPv6 ou IPv4, não é? É porque os projetos que estão mapeando o IPv4... projetos, por exemplo, o Shodan, que está escaneando IPv4, você tem Shadowserver escaneando, não é, varrendo todo o *range* IPv4. Os nossos *honeypots,* eles estão em IPv4, a gente está... o Klaus está trabalhando um pouco para a gente tentar conseguir migrar isso para v6, mas não tem muito software também em v6. Mas isso aqui são ataques todos em nível de aplicação, quer dizer, independe o que está embaixo, não é? Podia ser sinal de fumaça embaixo, com um outro

protocolo, mas se conseguir rodar Telnet, SSH, RDP, tiver um Mikrotik, não é--

SR. KLAUS STEDING-JESSEN: É. Isso, eu ia até comentar isso aí, Cris. Dependendo do ataque, o transporte é transparente, não é? Imagina para cima de um servidor Web, onde o atacante está, na verdade, usando o nome, se tiver um *quad-A* lá e for v6 para aquilo, para muitas ferramentas, o atacante vai ser meio que transparente, não é? Então, tanto faz como ele está chegando no servidor. E, depois disso, ele vai tentar um *exploit* para cima de um Wordpress ou vai tentar força bruta, etc., não é? Então, acho que dependendo... Nem todo ataque aí o pessoal acha que vai, necessariamente, envolver varreduras de v6, tá? Então, outra coisa para a gente ter em mente.

SRA. CRISTINE HOEPERS: Pois é. Bom, e se a gente for pensar aqui em... Espera aí. Toda vez que eu mexo aqui, sai o *mouse*. Em UDP, o que a gente mais vê? É SIP, tá? É voIP, e o que a gente vê é força bruta de credenciais em ramais voIP para fazer ligação para telefone convencional e para fazer... Quer dizer, todos aqueles serviços de centrais clandestinas de dados, toda aquela coisa de vender telefonia internacional mais barata é abusando dos ramais, não é, e das centrais telefônicas aí de muita gente. Então, SIP é, sim, o maior volume de ataques, não é, mas se a gente for olhar, o que são as outras portas UDP que o pessoal está procurando? Amplificação, tá? E aí, a gente começa a ter um link já com aquela parte de negação de serviço, não é? Tem bastante pergunta de negação de serviço, como evitar, tal. Negação de serviço, o ideal seria a gente ter uma Internet sem amplificadores e uma Internet em que todo mundo implemente... Klaus, me fugiu a palavra agora... completamente... A parte de *spoofing*, é *antispoofing*, não é? Que todo mundo implemente *antispoofing* aí. Então, eu acho que isso aí a gente tem que pensar que o pessoal, sim, está varrendo a Internet dia e noite, não é só o Shadowserver e o Shodan, procurando serviços que permitem amplificação, não é, e a gente vê aí os mais procurados: NTP, LDAP, DNS, SSDP, WS-Discovery, não é? A gente tem, como parte do acompanhamento lá do projeto... do programa Por uma Internet Mais Segura, acompanhado N outros protocolos, tá, e a gente tem notificado isso também.

Então, essa parte dos *honeypots,* do que a gente está vendo, bate muitos com nossos dados de amplificação. E aqui que tem um link do Shadowserver, tá? Para quem quer mais informações sobre Shadowserver, o link está aqui. Por quê? Porque o Shadowserver... eles têm um projeto já há muitos anos em que eles ficam varrendo a Internet por serviços vulneráveis, serviços que possam ser abusados, e uma das coisas que eles varrem a Internet é procurando por amplificadores, não é, e essa lista de amplificadores vai subindo, vai aumentando conforme a gente tem novos protocolos podendo ser

abusados, não é? O que tem nessa tabela que está disponível lá no site do programa Por uma Internet Mais Segura são os protocolos mais abusados aí no Brasil, não é? Então, a gente tem vários protocolos. Vocês podem ver que muitos batem com as portas UDP, que são as mais varridas aí, não é, e eu acho que é um problema hoje, que a gente não está conseguindo reduzir esse número de sistemas autônomos aí, que continuam com problemas, não é? A gente conseguiu reduzir bastante a parte de Ubiquiti aqui. Isso aí foi uma... A gente está tendo um retorno muito bom dos pequenos provedores tentando fazer essa redução, mas o número de servidores DNS recursivos abertos, não é, o número de SNMP permitindo acesso do mundo, NTP, SSDP, continua muito grande, não é? E a gente precisa reduzir isso aí, porque o poder de fogo está muito grande, e está muito óbvio, e está muito fácil fazer negação de serviço, não é? E eu acho que esse é um problema. Klaus, você tem comentários aí?

SR. KLAUS STEDING-JESSEN: É. É, só queria reforçar, pessoal, tenho certeza que todo mundo que está assistindo, muitos já receberam uma notificação nossa, do CERT.br, sobre este problema em particular, tá, problema de amplificação, não é? A gente manda semanalmente para milhares de ASs, a gente tem um esquema de rotação aí, não é, a cada semana um esquema, um protocolo diferente. Lembrando que a gente não usa cegamente os dados de *threat feed* nesses casos. A gente testa, tá, a gente retesta cada um deles para ter certeza que, naquele *timestamp* que a gente falou lá, informou no e-mail, o problema existia, o problema de amplificação, tá? E como a Cris falou, a gente está com números muito grandes, tá? Então, pega DNS: mais de 60 mil servidores são recursivos abertos, tá? Quer dizer, seria simples de corrigir isso, tá? Hoje em dia, assim, é trivial fazer isso em um Unbound, em um BIND9, etc., tá?

E aí, cai em um outro problema, a gente vai endereçar, tentar endereçar um pouco mais para frente, que é: quem está recebendo essas notificações hoje no seu provedor, tá? Então, é de extrema importância receber... Eu sei que chega muita coisa, então mais importante ainda é priorizar essas coisas. Então, eu pediria para todo mundo aqui priorizar essas notificações do CERT. A gente vai dar umas dicas de onde que a gente manda e-mail, como é que são nossos *headers* de e-mails aí para você poder filtrar isso, tá, e não é do seu interesse, do seu provedor, ter isso, tá? Você está gerando... amplificando ataques de terceiros, está jogando banda no lixo, está jogando reputação de IP no lixo também, tá? Então, tudo isso não é por ser o bom samaritano, tá? Quer dizer, isso está, também, impactando o seu negócio, tá? Então, não é... E outra: tem alguém, outro, detectando isso para você. Então, assim, você não precisa nem ter trabalho para tentar achar onde estão esses caras, tá? Então, assim, só reforçando isso daí, tá, Cris?

SRA. CRISTINE HOEPERS: Não, e aí reforçando... Eu já tinha visto isso no chat ali, o pessoal perguntando: "Ah, mas como bloquear NTP se UDP é 123?". Pessoal, diminuir amplificação não é bloquear porta na borda, não é, é lembrar que é configurar de maneira correta os serviços, tá? Então, eu acho que, assim, a gente sempre tem... a gente vê essa tendência na maioria das pessoas, elas querem resolver tudo botando filtro, não é? Na página do bcp.nic.br/i+seg, especificamente de NTP, tem lá, o mesmo texto, que é o texto que nós mandamos nas notificações, que é um texto que fala em você mudar a configuração, não é? Inclusive, nas notificações que a gente envia, tem lá qual o tipo de problema que tem de NTP e que tem de NDS (sic), e tem sugestões de como configurar corretamente, tá? Porque não é todo serviço que é bloqueio, Alguns você vai filtrar na borda, mas a maioria deles é configuração correta, não é, é configuração sem--

SR. KLAUS STEDING-JESSEN: Cris.

SRA. CRISTINE HOEPERS: Gerar uma resposta grande demais para uma pergunta pequena.

SR. KLAUS STEDING-JESSEN: É, isso bate justamente aqui, ó, Cris, tem alguém perguntando aqui, ó: "Sei que é pergunta de amador, mas o que seria amplificação?". Pessoal, amplificação é qualquer protocolo desses que permita uma resposta muito maior do que a pergunta e um protocolo que permite *spoofing*, como é o caso de UDP. Então, o que o atacante está querendo fazer para gerar um ataque de negação de serviço, tá? Ele '*spoofa*', não é, ele forja o IP de origem da vítima e manda um pacote para um desses serviços. Imagina que o pacote tem X bytes, só que a resposta vai ter 300 X, tá, vai ser 300 vezes maior, duas vezes maior, cem vezes maior, tá? Então, com isso, o atacante que antes conseguia gerar um ataque de negação de serviço, sei lá, de 1 megabit por segundo, agora, de repente, ele está conseguindo gerar 100 megabits por segundo, tá? E essa resposta vai para quem? Vai para a vítima, não é? Como o atacante conseguiu forjar esse IP de origem, a resposta vai para a vítima, que, de repente, começa a receber um monte de respostas UDP para algo que nunca perguntou, tá, vindo de múltiplas origens, certo? Tá? Então, como é que a gente corrige isso? Como a Cris já falou, um, mais fundamental de todos, é *antispoofing*, tá? Na sua rede, não pode ser possível gerar tráfego '*spoofado*', não é? E, segundo, corrigindo esses problemas, que são problemas de configuração, tá? Meu servidor DNS recursivo não pode receber perguntas do mundo, tá, ele deve apenas responder para aquelas redes previamente cadastradas, previamente confiáveis, tá? Então, eu acho que é basicamente por aí. Ah, legal, Cris.

SRA. CRISTINE HOEPERS: É, eu estava tentando compartilhar aqui. Pessoal, no site do bcp.nic.br, a gente tem um documento lá. Eu

estou aqui com milhões de coisas na tela tentando compartilhar aqui, mas a gente tem um documento sobre como reduzir, no bcp.nic.br, Boas Práticas, Redução de DDoS, tá, onde a gente explica essa parte de amplificação, não é, e que é exatamente isso que o Klaus estava falando. Aqui, nesse caso, é um gráfico que mostra como seria com DNS, não é, mas a ideia é exatamente essa, de que você tem um atacante, que ele consegue mandar algo muito pequeno para máquinas que são vulneráveis, não é, estão a serem abusadas, e essas máquinas respondem para a vítima com um volume muito grande.

E aí, um pouco em cima daquilo que eu comentei antes, não é, o que seria a Internet ideal? Seria uma Internet em que esses servidores DNS não fossem abertos, não respondessem, que servidores NTP não respondessem algumas *quares* específicas, não é, e é mais especificamente a parte acho que de... eu esqueci o nome dos dois comandos lá que replicam muitas vezes, não é? Olha, NTP consegue amplificar, a pergunta fica--

SR. KLAUS STEDING-JESSEN: *Monlist* é um deles, tem outros.

SRA. CRISTINE HOEPERS: É o *readvar* e o *monlist*, não é? Isso. Então, você tem... Alguns deles, o pacote que... A pergunta é do tamanho de 1 byte, a resposta vai ser 500 vezes maior. Então, é isso que é amplificação, não é? Você faz... E por que ela funciona? Porque o atacante está em uma rede que não implementa *antispoofing*. Então, assim, no fundo é muito importante todo mundo pensar em implementar *antispoofing*, porque enquanto a gente tiver redes que deixam sair pacotes '*spoofados*', ou seja, pacotes dizendo que são a vítima, em protocolos UDP, principalmente, você vai ter esse tipo de ataque indo direto para a vítima, não é? Então, até coloquei aqui. Lá no site do bcp.nic.br também a gente tem o programa Por uma Internet Mais Segura, não é, e se a gente for aqui na *home*, vocês vão ter... Aqui, olha, o programa Por uma Internet Mais Segura, e lá na parte de Ações Necessárias tem Contra Ataques de Amplificação, e que foi o que eu comentei, que para cada ataque, por exemplo, você tem aqui sugestões, olha: o *monlist* e o *readvar* permitem respostas maiores. E aí, aqui a gente tem dicas de como corrigir isso. Quer dizer, aqui já tem as dicas que são mandadas na nossa notificação também, que é exatamente o que você precisa colocar na sua configuração de NTP, não é? A gente tem vários documentos aí. Lembrar que tem alguns documentos do pessoal, que foi escrito pelo Eduardo, pelo Moreiras aqui, se vocês forem no Boas Práticas, *Antispoofing*, que explicam como fazer *antispoofing* e como ele funciona, como implementar com vários sistemas diferentes aí, tá?

Então, essa parte, voltando lá para os nossos slides de amplificação, não é, isso é o que a gente está notificando e o que a gente precisa. Quer dizer, a gente não pode... As nossas notificações,

pessoal, como é que elas são feitas? A gente, sim, vê no Shadowserver o que eles varreram tentando identificar como um serviço que permite amplificação, só que que nós refazemos esse teste, porque o Shadowserver, na verdade, assim, a porta está aberta, ele já classifica como permitindo amplificação; para nós, não. Por exemplo, não basta a porta 123 estar aberta, ela tem que estar respondendo ou *monlist*, ou *readvar*, e amplificando. Então, aí a gente vai notificar dizendo qual é o problema, como fazer e qual é o IP e com o *timestamp*. Então, mesmo que isso seja um roteador de banda larga... Que tem alguns modens aí de banda larga que vêm com NTP aberto, mesmo não precisando um servidor NTP naquilo lá. Então, assim, a gente tem esses desafios. Então, a gente tem um *timestamp*; se o IP for dinâmico, você vai ter exatamente a hora, sincronizado, a gente vai mandar para vocês para vocês poderem atuar em cima. Mas esse problema, ele está grande, não é, e bate com, voltando para o slide anterior, o que a gente está vendo nos nossos *honeypots*, o pessoal procurando isso, o pessoal está ativamente... os atacantes estão ativamente procurando isso daí, tá?

E falando um pouquinho mais dessa parte de ataques aqui no Brasil, não é, uma coisa que a gente queria comentar, assim, que já... E, graças a Deus, sequestro de rota, de ataques contra o sistema financeiro acalmou, mas já aconteceu, tá? E aí é que a gente fala assim, do tipo... você fica pensando que foi algo naquela linha da tecnologia espacial: como é que invadiram roteadores de borda? Força bruta de senhas, tá? Aquele foi um caso que até o Klaus falou que o pessoal comentou a senha Cisco123. Não, a gente teve um caso em que não era Cisco123, mas era "alguma coisa 123" a senha, e era uma empresa de consultoria que administrava vários provedores e que usava a mesma senha em todos os provedores, e tinha Telnet nos roteadores, e o atacante conseguiu ver que em um dos provedores era aquele consultor, e saiu, indo... e a gente teve, assim, vários dias seguidos em que cada dia era um cliente daquele consultor que tinha o seu roteador de borda invadido e que aí tinha um sequestro de rota de uma instituição financeira para tentar fazer os clientes daquela instituição irem para o local errado, não é? Aquela foi uma época, assim, bem complicada, e a gente viu outros que não eram relacionados com esse caso e que também era a mesma coisa, era força bruta de senha em roteadores de banda larga... em roteadores de banda larga, não, roteadores de borda que estavam de frente para a Internet, qualquer um do mundo conectava lá, maioria das vezes senhas fracas ou senha padrão do fabricante, tá? Então, assim, lembrar que senha padrão de Mikrotik era vazia naquela época, não sei se hoje em dia ainda é. Então, bastava o cara tentar lá dar *Enter*, ele estava no roteador de borda e fazendo sequestro de rotas, tá? Então, assim, de novo, não foi nada muito elaborado para invadir os provedores. Fala, Klaus.

SR. KLAUS STEDING-JESSEN: E só mais um comentário aqui, Cris, só exemplificando, não é, como você comentou. Uma vez que o cara... que o atacante comprometia esse equipamento aí que falava BGP, ele, então, anunciava um prefixo mais específico de uma instituição financeira, não é, e isso era, então... era anunciado aí para os seus *peers*, não é, que acabavam aprendendo essa rota mais específica errada, não é, o que nos remete, bom, primeiro, essa coisa... essa questão de, "bom, como assim, a única coisa era Telnet com senha e senha fraca", não é, mas também nos remete para boas práticas de roteamento, não é? O pessoal no chat mencionou uma hora aí MANRS, não é? Então, ser mais estrito com o que você aceita de anúncios, não é, e vai nos remeter também a RPKI, um negócio que nós vamos falar mais para frente um pouco também. Então, tem múltiplos problemas aí nesse caso que você descreveu, não é, mas assim, se a gente for pensar o mais básico, é assim: como assim um elemento seu de borda aceita Telnet do mundo e a única maneira de autenticação é uma senha, senha muito fraca, não é? Então, só para a gente ter isso em mente.

SRA. CRISTINE HOEPERS: É.

SR. KLAUS STEDING-JESSEN: E, de novo, a gente volta, como você falou, que não é *space-age*, não é? Assim, um negócio básico, mas que sim, acontece, não é?

SRA. CRISTINE HOEPERS: E até pegando uma pergunta, assim, alguém comentou aqui no chat: "Ah, SSH é mais seguro que Telnet". Com certeza, porque é cifrado, não é, mas em um caso como esse, se a senha é "blá-blá 123", e o cara chuta essa senha, não é, e a senha era o nome de uma pessoa 123, então, assim... E aí? Pode ter SSH. Se é só senha a única maneira de você proteger aquela conexão, ela pode ser quebrada, e é muito fraco, não é? Então, é pensar que assim... É que geralmente ele ver a(F) Telnet, isso é quase que nem crime com agravante, assim, entendeu, do tipo só tinha senha para proteger aquele roteador e ainda tinha Telnet habilitado, não é? Então, assim, é mais uma questão que piora um pouco. Até, Klaus, antes de a gente ir para o próximo, eu vi que tinha uma pergunta interessante de SIP, e eu acho que vale a pena a gente voltar um pouquinho, só--

SR. KLAUS STEDING-JESSEN: Uhum.

SRA. CRISTINE HOEPERS: Até esclarecer os nossos dados de *honeypots*. Os nossos *honeypots*, eles são máquinas que elas estão paradas na Internet, não é? O ideal, não é, em uma Internet ideal sem ataques, esses *honeypots* não viriam nenhum pacote, não é? Seria um tédio, a gente teria zero tráfego e a gente não estaria vendo absolutamente nada. O que a gente vê nos nossos *honeypots* são as ferramentas de atacantes e os atacantes varrendo a Internet e chegando no *honeypot*. Então, nesse nosso caso aqui não tem falso

positivo. Por quê? Porque não é um serviço legítimo aquilo ali. Aquilo ali... o que a gente está vendo é o que o atacante está chegando aqui, não é? Então, é diferente de a gente estar, nós, procurando um servidor de alguém e vendo se tem SIP ou não, até porque esse tipo de ataque que a gente está vendo... A gente escreveu um artigo um tempo atrás já falando o que a gente recomenda: senhas complexas nos seus servidores SIP, nos seus servidores voIP. Você vai precisar configurar isso uma vez. E o que a gente vê é que a maioria das instalações coloca números como senha dos ramais, coloca o próprio número do ramal como senha, você começa a ter servidores mal configurados, tá? Então, hoje, o que a gente recomenda é assim, se você tem isso, ele tem que estar bem configurado com uma senha forte, porque o que o pessoal está explorando são senhas. Klaus, você tem algum comentário adicional sobre SIP e voIP?

SR. KLAUS STEDING-JESSEN: Sim. Sim, justamente porque a pergunta falava assim: "Ah, mas é gerando falso positivo em *scan*", não é? Note aqui, pessoal, que isso aqui não tem nada a ver com *scan*, tá? Isso aqui tem a ver com, a Cris falou, um *listener*, ou seja, um sistema que emula um servidor SIP. Nesse caso, a gente emula um Asterisk, tá? Ou seja, esse emulador fala o protocolo SIP. Então, não basta dizer que: "Ah, sim, estou escutando na porta 5060". Não, ele tem que interagir, ele tem que falar o protocolo e tem que avançar a um ponto em que ele quer se autenticar em um ramal, e a gente vai além, a gente forja uma resposta dizendo: "Sim, sim, você está autenticado no ramal. E agora, o que você quer fazer?" E aí, você consegue ver o passo além, você vê as ferramentas querendo dar um *invite* de SIP, não é, ou seja, originar uma chamada, tá? E aí, você consegue 'logar', inclusive, para que telefones seriam essas chamadas, tá? Nesse artigo que a Cris comentou da *;login:*, não é, aquela publicação da Usenix, a gente, inclusive, levantou que na época, assim, muitas das chamadas era para a URA do Bank of America, por exemplo, claramente com o objetivo de fazer fraude, não é, do ponto de vista do atacante, sem pagar uma ligação internacional, porque quem vai pagar isso aí vai ser a organização que tem esse Asterisk ligado na rede e na linha telefônica, não é? Então, assim, a gente conseguiu ver várias coisas interessantes nesse sentido. Então, só para deixar claro que não estamos falando de varreduras, tá, estamos falando de conexões de fato e interações com protocolos reais, tá?

SRA. CRISTINE HOEPERS: É, é isso aí. Então, só... eu achei que valia esclarecer, porque podia ter ficado uma confusão, que no nosso projeto de *honeypots* a gente não varre ninguém, tá?

Já nessa parte de estatísticas de amplificadores, como eu comentei, nós aqui, como CERT de responsabilidade nacional de último recurso, nós conseguimos acesso lá no Shadowserver a todos os dados relativos a sistemas autônomos alocados ao Brasil, a IPs alocados ao

Brasil. Então, nós temos esses dados, mas a gente não confia cegamente exatamente, porque pode ter falso positivo, não é? Então, o nosso cuidado para não ter esses falsos positivos é muito grande. E é por isso que nesse caso, a gente, de certa forma, usa os dados do Shadowserver como uma semente, a gente retesta, e aí gera um *timestamp* bem específico nessa área aí, e aí consegue dar essa parte.

Pessoal, eu vi que tem bastante pergunta começando a aparecer, sobre boas práticas de SSH, não SSH, como fazer. A gente vai ter slides que a gente vai discutir isso em detalhes e vai ter sugestões exatamente do que fazer e o que é mais efetivo para prevenir essa parte de força bruta de senhas e de acesso remoto, porque, sim, todo mundo precisa ter gestão remota, não é, do seu parque, você precisa poder administrar remotamente, você tem o seu parque em várias cidades, você tem... Então, assim, a gente vai comentar isso um pouco mais para frente, não é? Agora, a gente está querendo reforçar um pouco onde estão os problemas, porque... até para vocês entenderem o que as soluções podem resolver, não é? Determinadas soluções resolvem alguma parte do problema, mas não outra, tá? Então, eu acho que é isso que a gente quer discutir um pouco mais, essa parte de problemas, não é? E o que a gente quer até comentar é que força bruta de senhas também é usada em cima dos roteadores domésticos, não é, para... E lá o objetivo é o quê? É também desviar tráfego, mas desviar para trocar o servidor DNS desses modens de banda larga. Esse é um ataque que a gente vê desde 2014 acontecendo, tá? Não é nada novo, mas ele continua, não é? Como é que o pessoal faz essa força bruta de senhas? Ou é via Telnet... mas aqui os ataques CSRF, ou seja, você faz um JavaScript malicioso, coloca em um site legítimo... isso já aconteceu, de você ter sites de notícias, blogs, muito lugar que o pessoal consegue ver uma vulnerabilidade, no Wordpress ou em alguma coisa, colocar um JavaScript malicioso, e a pessoa está na casa dela acessando aquele site para ler uma notícia, e esse JavaScript faz o quê? Força bruta de senha no roteador a partir da rede doméstica, tá? Então, assim, esse é um caso que não adianta você dizer: "Ah, mas ninguém pode acessar o meu... o modem do meu cliente da Internet". Mas se o cliente está acessando o modem internamente, eles também estão fazendo força bruta de senhas, tá? Então, por isso que para quem está acompanhando aquelas discussões que tiveram no Lacnic, no GTR, não é, a BCOP, que foi escrita lá, o LAC-BCOP, que foi do LACNOG junto com o M3AAWG, não é, aquela ideia de que tem que ter uma senha única complexa para cada roteador de banda larga, porque tem muitas maneiras de você fazer força bruta de senhas; lembrar que o que eles querem é alterar esse DNS para te mandar para um site falso, não é?

E que tipo de site falso? É tudo, não é? A gente pensa... Começou com bancos, mas hoje em dia a gente tem vários serviços de pagamentos. Hoje, eles estão fazendo, sim, muito para serviços de

streaming, de mobilidade, ou seja, toda a parte de aplicativos, como Uber, como iFood, redes sociais, Webmail, comércio eletrônico. Quer dizer, a gente vê de todos esses tipos de domínio. Muitas vezes, é para te mandar para uma página falsa para te induzir a baixar um *malware,* outras vezes é realmente uma página de *Phishing* para pegar credenciais, tá? E aqui, a gente tem várias páginas... Hoje, a gente teve uns blogs que nós escrevemos em conjunto com o pessoal do Team Cymru explicando em inglês como funciona esse ataque, porque a maioria dos servidores DNS, que são os maliciosos, são hospedados fora, não é? Teve um post bem interessante aqui do pessoal explicando como é que funciona o CSRF. Ele é passo a passo essa parte do ataque via *cross-site request forgery*, tá? Então, assim, é bem interessante. E a gente queria deixar claro que isso daqui não é *domain hijacking*, não é *cache poisoning*, não é envenenamento de *cache*, não é um servidor DNS invadido, não é? O que a gente tem são servidores DNS levantados em *clouds*, qualquer uma, e que respondem de maneira autoritativa por esses domínios aqui, que são das organizações vítimas, não é, e para o resto do mundo eles são recursivos abertos. Então, a experiência do seu cliente não vai ser comprometida, o seu cliente vai continuar acessando a Internet, resolvendo normal todo o resto, só que, para alguns domínios, ele vai para o lugar errado, não é? Klaus, você tem algum comentário adicional aqui?

SR. KLAUS STEDING-JESSEN: É, eu só queria reforçar essa parte, Cris, que, assim, é extremamente importante essa questão de semântica, tá, porque assim, tem tanto ataque diferente envolvendo DNS. Então, é importante ser preciso nessa hora, não é? Então, não, não é *cache poisoning*. Por que não é *cache poisoning*, pessoal? Porque nós estamos falando de respostas com autoridade, não é, e para isso, o atacante, ele, explicitamente, levantou e configurou um servidor DNS com autoridade. Nessas horas que é importante a gente ter bem claro na nossa cabeça, assim, o que... qual é a diferença entre um DNS recursivo e autoritativo, não é? Nesse caso, ele... E outra, ele está usando infraestrutura, em geral, de *cloud* por aí, tá, usando cartões furtados etc., ele vai lá calmamente, levanta uma máquina virtual, coloca lá um servidor DNS, e esse servidor DNS, como a Cris falou, ele é recursivo para qualquer coisa, tá? Então, sim, ele resolve nomes, mas para algumas zonas em particular, de banco, etc. e tal, Netflix, coisas populares, ele responde com autoridade, obviamente, errado, não é, e resolvendo para um IP que ele tem controle, não é? E lá, obviamente, vai ter uma página de *Phishing*, vai ter algo que explore aí o usuário, tá? Então, é importante isso aí, e outra coisa, quando a gente for falar de ter, vamos dizer, uma telemetria, saber o que está acontecendo na sua rede, você vê trivialmente com o *netflow* que você poderia... nós vamos ter um exemplo disso vendo... Ok, tira os acessos legítimos de DNS da minha rede e me mostra o resto, tá? Se você tem um cliente seu que está fazendo uma consulta DNS para um servidor,

é algo que você não espera, não é? Você tira todos os Googles da vida, o seu próprio recursivo legítimo, etc., e tem um 'IPzinho' lá que está lá na UVH, não é, sei lá onde, é suspeito, tá? E você faz isso com uma consulta de *netflow*, tá? Então, é nessas horas que ter, vamos dizer, visibilidade do que está acontecendo na sua rede é importante, tá? A gente vai voltar nisso daí só para reforçar esse ponto.

SRA. CRISTINE HOEPERS: Sim. Eu acho que é bem importante falar isso, porque a gente vai comentar sobre como detectar essas coisas, como detectar se tem negação de serviço saindo da sua rede, que acho que é relacionado com uma pergunta que chegou aí de como impedir ataques saindo da rede, não é? Quer dizer, parte é reduzir a quantidade de serviços seus que estão permitindo amplificação, é implementar *antispoofing*, não é, e, depois, a gente vai falar um pouco sobre como detectar *botnets* dentro da sua rede e tentar--

SR. KLAUS STEDING-JESSEN: E outra coisa, não é, Cris, a gente vê muito provedor, assim, pequeno e médio, em que ele só fica sabendo que está participando de um ataque de negação de serviço, ou recebendo, enfim, quando começa a vir reclamação de usuário, não é? "Ah, mas a Internet está lenta", não é? E o que a gente está reforçando aqui é que você tem que descobrir isso antes, pessoal, não é, antes de... Você não pode depender de usuário dizer que está lento, não é, até porque pode estar lento por N motivos, não só ataque de negação de serviço, mas você tem que estar... ter as ferramentas já previamente configuradas para que, qualquer coisa que saia do seu normal, você consiga ver, não é? Então, assim, a primeira coisa... antes de sair mitigando algo, você tem que descobrir que existe algo, não é? Então, acho que esse é outro ponto para a gente reforçar bem aí.

SRA. CRISTINE HOEPERS: Inclusive, pessoal, aquele documento de recomendações contra DDoS que tem lá no bcp.nic.br e foi escrito pela gente aqui do CERT, o maior foco daquele documento é como a sua rede não gerar DDoS, tá? Então, assim, vocês vão ver que a maioria das recomendações que a gente tem é como evitar que saíam ataques de negação de serviço, e aí uma parte bem grande disso que o Klaus falou agora, como instrumentar a sua rede para medir se está acontecendo um ataque ou não, e aí tentar conseguir partir para uma mitigação, porque a gente também vê muita gente que tem dificuldade para mitigar ataques chegando porque não está conseguindo medir exatamente que tipo de ataque é, como que é o *payload* desse ataque, como que ele está acontecendo, não é? Então, assim, isso também é importante para se prevenir de ataques contra a sua rede, não é?

E aí, uma coisa que a gente queria... não é, meio que resumindo o que a gente está vendo aqui. Se a gente for pensar hoje em

incidentes que a gente está vendo, em coisas que a gente conversa com redes que estão acontecendo incidentes, ou que a gente está acompanhando em vazamento de dados, o que a gente realmente vê é força bruta de senhas. Isso, hoje, está sendo o número 1, tá? De tudo, de e-mails, de serviços em nuvem... Isso quando você não tem o negócio totalmente exposto, sem senha nenhuma, não é? Então, assim, muito a tentativa... muitos comprometimentos de senha para acesso remoto e gestão remota de ativos de redes de servidores. A gente está vendo muito essa parte de vulnerabilidade, exploração de vulnerabilidades conhecidas, ou seja, muito antigas e tudo completamente sem *patches*, tá? Uma estimativa que a gente tem é que, olha, mais de 80% do que a gente vê hoje, é bem Pareto isso aqui mesmo, seria resolvido aplicando *patches*, cuidando com erros de configuração: "Ah, eu achei que eu tinha levantado *firewall* e não levantei", "ah, eu achei que eu tinha configurado a máquina da *cloud* com a segurança tal e não tinha ido", "ah, eu levantei tal coisa e não funcionou", tá, e se tudo tivesse segundo fator e múltiplo fator, tá? Na Conferência do FIRST esse ano teve um painel onde tinham vários especialistas de segurança e no... era até para discutir a profissão de segurança como um todo, mas, no final, eles perguntaram para os painelistas o que eles achavam que as empresas... se elas pudessem melhorar uma coisa, fazer o quê, não é? A Katie Moussouris, que é bem conhecida nessa área de *pentest*, foi ela que criou os primeiros conceitos de *bug bounty*, não é, quer dizer, de você tentar pedir que pessoas ataquem a sua rede, tentar fazer... pagar para quem descobrir vulnerabilidades no seu serviço, quer dizer, a especialidade dela é *pentest*, e ela falou assim: "Olha só, vocês querem melhorar, acabar com *ransomware* e melhorar, assim, muito a segurança de todas as redes? Segundo fator em tudo". Assim, foi resumo dela, ela falou assim: "Olha, hoje, a gente está invadindo as coisas via senha, serviços que só têm senha. Ponham segundo fator em tudo". Então, acho, assim, não é uma visão só nossa, não é? E é focar no básico, tá? Eu diria, assim, é *patches* e *hardening*. Não, não pode deixar coisas abertas, serviço levantado que você não vai usar, porque aquele serviço levantado que você não vai usar é o que você vai esquecer de aplicar *patches*, é o que vai ter uma senha que você nem se tocou que estava lá, não é? Proteger tudo e adotar alguma maneira de autenticação múltiplo fator, não é, seja um aplicativo autenticador, seja um *token*, não é, como o Yubikey. A gente pensar... que eu acho assim, tem muita coisa simples a fazer, e até mais para frente o Klaus acho que vai comentar um pouco, nem que seja SSH com chave criptográfica, mas tem que sair da senha como autenticação dos serviços, tá? Isso é... e principalmente os serviços que são *core* das redes de vocês, toda a parte de ativos de rede, toda a parte de roteadores, não é?

SR. KLAUS STEDING-JESSEN: Cris, eu acho que assim, a gente sairia aqui com missão cumprida, não é... eu diria assim... A gente brinca aqui no CERT, pessoal, assim, o ano é 2021, tá? Assim, lembrar isso aí. O ano é 2021, não tem mais que usar senha, tá? Assim, segundo fator de autenticação em tudo que puder, tá? "Ah, mas eu tenho coisas legadas". Ok, mas e o resto? Tá? "Ah, mas eu não tenho grana para comprar Yubikey para todo mundo". Tem soluções mais simples, tem desde, como a Cris falou, o aplicativo autenticador. Lembrando, o próprio Registro.br, antes de suportar *token*, tinha, há anos, aplicativo autenticador, leia-se um... tem N apps que fazem isso, tá; o SSH com chave criptográfica, tá? Então, assim, se desse para passar uma... assim, um *takeaway*, não é, uma lição aqui para guardar, pessoal, dessa apresentação é essa questão de multi... MFA, tá, ter múltiplos fatores de autenticação, tá? Isso, eu acho que, assim, seria... metade dos seus problemas vão embora, assim, na hora.

SRA. CRISTINE HOEPERS: Com certeza. E eu até diria assim... Tinha alguns comentários aqui interessantes no chat, alguém colocou ali: "Ah, mas em geral eles não acreditam que tem alguém querendo atacar a senha", não é? Não acredita... Então, mostra esse vídeo aqui para a pessoa que não acredita que os atacantes estão atacando senhas, porque a gente ficou até agora tentando mostrar que é isso que as pessoas estão fazendo, e não, não é assim que ela pensou: "Que interessante esse provedor". Não, eles saem varrendo a Internet, dia e noite, todas as portas, procurando se tem algum serviço, um *banner* de autenticação, e vai ser força bruta de senha. E hoje, uma coisa que o pessoal chama lá fora de *credential stuffing*, o que eles vão fazer? Você tem todos esses bancos de dados de vazamento de senha, e aí eles usam aquilo também para tentar adivinhar senhas em serviços assumindo que alguém vai reutilizar senha ou que lá tem alguma senha que pode já ter sido usada alguma vez, no serviço e vai ser usada em outro, tá? Então, assim, acontece. Isso é, hoje, o que é mais explorado, não é?

E eu vou passar agora para o Klaus assumir os slides daqui para frente, a gente vai inverter quem dá palpites em quem, mas falar, assim, o que priorizar, não é? Eu acho que o começo é essa parte mesmo de senhas, mas é o que priorizar agora.

SR. KLAUS STEDING-JESSEN: Pessoal, como vocês já viram aí, a gente falando bastante, de novo: tentar encarar esses problemas como uma ótica aí de Pareto, 80/20, não é? Onde que eu vou investir o meu esforço aqui para ter o maior resultado? Este slide aqui, pessoal... Assim, se todo mundo saísse daqui com essas três colunas implementadas, tá? Então, primeiro, absolutamente necessário manter sistemas atualizados, tá? E, de novo, aquela história, não é o *exploit*, o *zero-day*, tá, que só a agência do governo XPTO tem, tá? Não, a gente está falando de CVEs antigos, de coisa de um ano, tá? "Ah, mas

não foi feito *patch*". Aí tem N, N motivos, tá? "Ah, porque eu não sabia que tinha essa máquina no parque", "ah, porque eu precisava de uma versão antiga de Wordpress, porque tinha uma extensão que todo mundo usa e que não dá para atualizar", tá? Então, tem N motivos, a gente sabe que, assim, que... Outra: o volume de máquinas é grande, mas aí precisa priorizar, tá? E outra coisa que a gente vê muito: "Não, não, mas essa máquina aqui não precisa atualizar, porque ela está só na rede interna", tá? E é nessas horas que a gente vê grandes comprometimentos com esquema de movimentação lateral, não é? Uma vez que o atacante entre em uma máquina da rede interna, por que muitas vezes é tão fácil essa movimentação lateral? Porque dentro da rede da pessoa é um queijo suíço, tá, em parte por essa filosofia do "não, não, mas na rede interna não precisa, não é, pessoal?". Então, assim, não tem essa de rede interna *versus* externa, todas as máquinas precisam seguir essa filosofia aí de manter atualizado. Não sei se você quer comentar um pouquinho, Cris, rapidamente de CVSS--

SRA. CRISTINE HOEPERS: Pois é.

SR. KLAUS STEDING-JESSEN: Como é que você poderia priorizar um pouco essa aplicação de *patches*.

SRA. CRISTINE HOEPERS: Uma coisa que eu acho, assim, que é uma recomendação para todo mundo é: vocês não podem cair no pensamento do "ah, mas é impossível aplicar tudo, então eu não vou... jogo mãos para o alto e não vou fazer nada, então, porque não consigo fazer tudo". Não, é priorizar. Você começa priorizando tudo que é o crítico da tua organização, e aqui a gente falando muito em como.... o contexto aqui da Semana de Capacitação para provedores, não é, a gente está falando de roteadores, dos principais servidores, de toda a questão de ativos de rede, não é, tudo o que você usa para o seu provedor funcionar, mas isso vale para empresas também. Você vai definir o que é o principal, mas aí dentro desse principal você tem que definir o que eu aplico *patches* primeiro e o que é mais importante priorizar. Hoje, a gente tem... a maioria dos *advisors*, dos alertas dos fabricantes, eles já vêm com uma nota de CVSS, não é, que é o *Common Vulnerability Score*, e aí você, em cima desse *score*, consegue priorizar algumas coisas, tá? Então, pensem, olhem, vejam o que o fabricante põe, se é... principalmente o que é: é uma vulnerabilidade remota, uma vulnerabilidade local? Mas aí, além disso, se vocês forem lá, tem calculadoras onde você pode responder um questionário do seu ambiente de criticidade, de como é usado, e aquilo vai te dando uma nota de se aquela vulnerabilidade é muito importante ou não para instalar... para aplicar, mas tentem pensar em priorizar, não é, porque... Inclusive, tem uns trabalhos novos que foram apresentados na última conferência do FIRST, e tem um novo padrão, que é o EPSS, quem sabe se, no final, se sobrar tempo... a gente quer deixar um bom tempo para perguntas no final, mas a gente pode falar disso, que é o

uso de métodos estatísticos que eles estão, inclusive, conseguindo com uma boa... com um erro ali de 5% só, quer dizer, 95% de acerto, quais vulnerabilidades que vão ser exploradas e que vão se transformar em algo que possa virar um [ininteligível] e virar um *malware*, tá? Então, assim, a gente tem que começar a focar naquilo que é mais importante, não é? Eu acho que isso é muito importante, e tem ferramentas que podem ajudar vocês a priorizar no que instalar *patches* primeiro ou onde focar isso daí.

SR. KLAUS STEDING-JESSEN: E aqui, a coluna do meio, pessoal, eu acho que, então, como a gente já falou várias vezes aqui, acho que é o mais importante dessa apresentação. Assim, temos que mover para um esquema que não seja apenas senha, tá? Isso vale para tudo, tá, mas nesse contexto, obviamente, de provedores, estamos falando dos seus elementos de rede, tá, estamos falando dos seus servidores importantes, tá, do seu provedor, estamos falando do *desktop* do analista. "Ah, é só um *desktop*". Sim, mas é o *desktop* que dali ele gerencia todos os seus equipamentos de rede, tá? Então, também é importante, tá? "Ah, mas eu não tenho grana para comprar Yubikey para todo mundo". Tem N, como a gente comentou aqui, possibilidades, tá? Chaves criptográficas, tem app que dá para fazer por software, tá? Então, eu acho que essa é a principal mensagem. Tem alguém que perguntou aqui: "Ah, mas se vazou, a chave SSH também já era". Bom lembrar que a chave, ela pode ser protegida por uma *passphrase*, tá? Muita gente acha, necessariamente, que porque tem uma chave, então, o cara põe um *passphrase* vazio. Sim, ele pode ser útil para automatizar certas tarefas, não é, 'logar' em servidores, fazer certas atividades via Kron(F), por exemplo, mas aqui nós estamos falando de proteger essa chave com uma *passphrase*, tá? Então, imagina que é uma chave sua, que você usa para uma sessão interativa em elementos de rede ou servidores, então ela vai estar protegida por um *passphrase* também.

E outra coisa é pensar que assim, pessoal, a gente não pode, vamos dizer, congelar o que a gente vai fazer na linha do: "Ah, não, mas é possível de dar errado". Bom, tudo é possível de dar errado, não é, o que a gente não pode acho que é reverter, então: "Ah, eu logo(F), então vou continuar usando senha", que é péssimo, tá? Então, acho que é questão de medir também, assim, em uma escala do que protege o quê.

E por fim, pessoal, acho que outra coisa é muito importante, tá? De novo, a gente está falando, assim, que... não estamos falando em tecnologias do além, em gastar milhões em *appliances* e *machine learning*, isso e aquilo, quando, na verdade, na prática, pessoal, a maioria dos comprometimentos ou problemas sérios vão ser descobertos por terceiros, tá, como nós, por exemplo, do CERT. A gente... como eu comentei, a gente notifica milhares de ASs toda

semana, tá? Como é que a gente faz isso? O bom e velho Whois. A gente vai olhar lá: Ah, o AS X, tá? Ah, qual que é o *abuse contact* dele? Ah, o e-mailzinho tal. A gente vai mandar e-mail reportando o problema, não é? E aí, não passa um dia, pessoal, sem a gente escutar aquela história do: "Ah, mas esse e-mail ninguém lê". "Não, não, não, esse e-mail chega muito *spam*, então isso aí vai direto para a caixa de *spam*", tá? Sim, eu não estou dizendo que é fácil, tá, sim, tem bastante lixo que entra nessas caixas, mas é importante priorizar isso daí. Tem alguém lendo? Tem. Como é que vai priorizando? Ah, prioriza, por exemplo, por origem. Hoje, a gente vai dar umas dicas, começa lendo as coisas do CERT.br primeiro, tá? Tem N organizações grandes, pessoal, que ficaram comprometidas por meses, tá, e que tinham um investimento grande em segurança, e, um belo dia, como é que eles descobriram do comprometimento.... ficaram sabendo desse problema? Via um terceiro, que falou: "Olha, estranho, eu estou vendo um tráfego aqui sendo originado da sua rede. Você tem certeza que está tudo bem aí?". O cara mandou e-mail, tá? É gratuito isso aí, pessoal, tá? Então, outras organizações vão ter dados relevantes, tá, e é gratuito. Então, começa olhando isso daí, tá? E essa é a dica que a gente teria. Você teria alguma coisa a adicionar aí, Cris, nessa parte de receber notificações?

SRA. CRISTINE HOEPERS: Não, acho que mais para frente a gente vai até botar um exemplo de notificações, mas, de novo, é um lugar onde eu vejo muito o pessoal falando: "Ah, mas a gente recebe muito e-mail, então eu ignoro tudo". E essa é uma das coisas que a gente vai discutir um pouco para frente, que o segredo disso é triagem, e você priorizar parceiros que estão mandando informações relevantes e tratar isso primeiro, não é? Você não pode simplesmente abandonar, não é? Eu vi muita gente dizendo: "Ah, pessoal, tem que monitorar as coisas". Sim, vai ter muito *Log*, e aí o segredo é saber o que monitorar, não é? Eu acho que é importante a gente pensar nisso, e priorizem. Vocês podem ter coisas, assim, que podem salvar o dia em um incidente grave chegando nos e-mails de vocês e vocês estão perdendo isso, não é, porque entra naquela linha do: "Ai, é muito e-mail, então não vou nem olhar", tá? Não encarem assim. A gente vai, pelo menos, dar umas dicas de como priorizar os nossos e-mails do CERT, que sempre vão ter *Logs*, *timestamps* e dicas de como resolver o problema, tá, que eu acho que é importante também.

SR. KLAUS STEDING-JESSEN: Acho que podemos avançar, então, não é, Cris? Bom, só reforçando, então, algumas boas práticas aí para acesso remoto. Bom, esse aqui a Cris já comentou, não é, quer dizer, jamais utilizar senhas padrão ou de teste, tá, usando um padrão, assim, muito conhecido: "Ah, é o nome do provedor 123, é o nome do consultor 123", tá? Senhas fortes; já falamos N vezes, não é, autenticação de dois fatores. Outra coisa, pessoal: Ah, um sistema

legado que só permite senha. Bom, aí você aumenta a monitoração, tá? Quem está conectando nessa máquina? De onde? Você pode fazer um Kron(F) simples, que te manda um relatório diário, tipo, quem são... de onde estão vindo essas conexões, não é?

No caso de SSH, acho que a coisa mais importante, pessoal, tem N coisas aí complementares, mas é primeiro par de chaves, tá? Assim, essa é a primeira coisa a fazer, tá? Você pode complementar isso de N maneiras, tá? Bom, reduzir equipamentos que tenham... que permitam SSH de frente para Internet; você pode filtrar por origem, tá? Eu tenho uma origem bem definida aqui, uma rede minha de gerência. Bom, então eu só aceito SSH dessa rede de gerência, ponto, tá, além do... Então, tudo isso aqui, pessoal, é complementar àquele primeiro ali de acesso com par de chaves, tá? Então, eu queria que o pessoal saísse daqui sem... não usando mais SSH apenas com senha, tá? Então, filtrar por origem. "Ah, eu quero mudar a senha... a porta padrão para uma outra que não seja padrão". Ok, pode até ser interessante até para reduzir o volume dos seus *Logs*, para olhar, mas não usem isso como única... como solução, tá, até porque, independente da porta que você colocar, você vai ter força bruta SSH, tá? Você pode acreditar nisso aí, tá? Outra coisa: considerem fazer um *gateway* de autenticação, chame isso como quiser, tá? Tem gente... não é, um *jump host*, *host* de... um servidor de salto, ou *host* de salto, etc., ou seja, uma máquina que você faz um SSH para lá e de lá você consegue, então, acessar os seus elementos de rede, por exemplo, tá? Apenas de lá, não é? E, de novo, essa é a ideia de ter aí o conceito muito bem definido de uma rede de gerência, tá? Esse negócio não pode estar aberto para Internet, qualquer um acessa o meu Mikrotik aqui, de qualquer lugar, tá? Então, isso tem que ser uma coisa bem definida também. Outras recomendações nesse link, tá? A gente tem um *white paper* bacana aí na nossa página. Outra coisa: você pode complementar... além de par de chaves, você pode ir além, pessoal, tá? Aqui no CERT, por exemplo, a gente, além de par de chaves, você tem que botar uma *passphrase* para liberar essa chave, além disso, a gente ainda usa Yubikey. Você tem que espetar um dispositivo físico, tá, para poder--

SRA. CRISTINE HOEPERS: Klaus, para quem não souber o que é Yubikey, é um dispositivo físico mesmo, não é, e você tem que ter um dedo aqui, tem que ter um contato, tal, não adianta estar abandonado. E eu acho, assim, só porque tinha um pessoal: "Ah, mas alguém pode roubar a chave criptográfica". É aquilo que o Klaus falou, sim, tudo pode dar errado, não é? Alguém pode invadir o *notebook* que você estava usando, roubar a chave criptográfica, descobrir a conferência em que você vai, mão leve, pegar o Yubikey do seu bolso, tal, mas você concorda que é muito mais difícil e mais complexo de fazer? Porque ele vai ter que conseguir tudo isso e mais algo físico. Então, assim, hoje está muito fácil usar essas coisas, pessoal. Então,

assim, não se limitem. Pensem, sim, em ter um *gateway* de autenticação, ou seja, essa máquina, que aí você não precisa comprar cem Yubikeys, não é? Vai ser para o pessoal que gerencia esses dispositivos mais chave, vai ser quem gerencia os servidores, não é? E aí, você fazer esse *gateway,* ter a segurança maior e ter uma parte aí, não é? Mas era só complementando, dada umas perguntas que eu vi no chat, não é? O pessoal sempre... Sim, sempre tudo pode dar errado, mas é que nem a segurança da nossa casa, não é? O cara que vai entrar, ele olha: "Putz, essa aqui tem uma grade, tem câmera, tem tal coisa, tem isso, tem aquilo, acho que eu vou para a do lado", não é? E aí, claro, se alguém chegar com um caminhão tanque, ele vai derrubar a grade e entrar na sua casa, mas aí depende também do esforço que vai fazer, mas hoje está muito fácil, não é? Era um comentário adicional sobre isso, Klaus.

SR. KLAUS STEDING-JESSEN: Não, maravilha, Cris, muito bom. Bom, então essa acho que é uma parte bem crucial nessa parte de acesso remoto, não é? Então, assim, pensar em algum mecanismo de segundo fator, tá? Então, eu acho que, assim, isso seria muito importante considerar. [Se quiser avançar aí, Cris.]

SRA. CRISTINE HOEPERS: Espera aí que... Foi!

SR. KLAUS STEDING-JESSEN: Tá. Então, assim, só relembrando, pessoal, muito simples, tá? A gente quis... Sim, a gente quer pausar, sim, só o último slide. A gente vai fazer um 'breakzinho' rápido. Só o último slide aqui, só para relembrar como é que a gente gera--

SRA. CRISTINE HOEPERS: São os últimos três, Klaus. Os últimos três.

[risos]

SR. KLAUS STEDING-JESSEN: É. Tá bom. Então, com *ssh-keygen*, nesse caso eu estou gerando especificamente uma chave ed25519, tá, pessoal? "Ah, mas o meu *Switch* não suporta esse tipo de chave". Ok, você pode gerar uma chave RSA, tá, mas hoje, se você puder escolher, esse eu acho que é uma boa recomendação, tá, uma chave bem interessante. Você, então, nesse exemplo você passa um caminho onde você quer gerar essa chave. De novo, ele é um par de chaves, tá, pessoal, uma chave privada e uma pública. Nesse exemplo, você pegaria a porção pública, tá, na linha de baixo ali, o servidor *underscore* tal, tal, tal, .pub, e colocaria no *authorized keys* do usuário que você quer 'logar' nesse servidor remoto, tá? Nesse caso, nesse exemplo, você iria 'logar' como *root*, mas poderia ser em qualquer usuário. Mesma coisa para elementos de rede, tá? Você pegaria essa porção aí pública e colocaria lá. Só quem detém, então, essa chave privada, que foi gerada nesse exemplo acima aí, conseguiria, então, 'logar'. O -C ali é só um comentário, pessoal, você poderia ter múltiplas

chaves dessas, cada uma com um comentário: "Ah, essa aqui é do servidor A, essa aqui é do B, essa aqui é do roteador tal", tá? Muitas vezes, você vai querer ter uma chave sua, pessoal, aí você bota um e-mail, o seu nome, enfim. É um comentário qualquer, tá?

E aí... Então, assim, por exemplo, como eu faço isso em uma máquina Windows? Tem um exemplo aí com PuTTY, tá, muito popular também, também você consegue gerar chaves ed25519, tá? Outra: escolha uma senha forte, um *passphrase* de fato para proteger essa chave, tá? É mesmo esquema. Então, você pode fazer... Isso é muito comum, não é, às vezes, o cara tem uma... Eu preciso de uma máquina Windows, por exemplo, como cliente para 'logar' nesse seu servidor SSH, não é? Então, tranquilo, você pode fazer com Windows também. MAC tem isso também, sem problemas.

E uma recomendação... Quer dizer, no seu *sshd_config*, não é, quer dizer, no seu *daemon* SSH rodando aí no servidor, você vai lá e diz assim: Olha, eu... Você proíbe, por exemplo, autenticação por senha, tá, então, autenticação por *pubkey*, *yes*; *password*, *no*, tá? Você pode ser explícito, você pode ser específico, por exemplo, para a conta de *root*, você diz que não pode *password*, não é, mas precisa de... mas, por exemplo, com *pubkey* é permitido, tá? Então, de cara, pessoal, essa configuração aí, todas as... pelo menos as ferramentas automatizadas que a gente tem visto por aí, tá, *malware* e força bruta de SSH, de cara já não funciona com essa configuração aí, porque ele espera poder fazer força bruta de senhas. Então, isso daí já está... você já está fora do radar, pelo menos, dessas ferramentas, tá? Então, esse é um... Não sei se você quer complementar aí, Cris, nessas configurações.

SRA. CRISTINE HOEPERS: É. Eu acho que, assim, o importante, pessoal... Não tem muito mais o que recomendar, não é, mas é que se você sai do que está todo mundo explorando, que é senha direto, você já sai do normal. Eu lembro que teve uma pergunta só que a gente acabou não falando, alguém: "Ah, vocês recomendam mudar de porta?", não é? Os atacantes vão acabar achando se você colocar em uma outra porta, mas a nossa experiência é: a porta de SSH, a quantidade de *Logs* é tão grande, tão grande, que fica difícil você, às vezes, identificar ataques com sucesso ou outras coisas, tal. Então, às vezes, você só botando em uma outra porta, aí você consegue monitorar um volume menor e você tem vantagens do outro ponto de vista, mas não que ninguém vai achar mudando de porta. Então, não achem que mudar a porta do servidor vai proteger vocês de maneira aí, não é?

SR. KLAUS STEDING-JESSEN: E outra coisa, Cris, o pessoal falou muito do Fail2ban, não é, ou seja, de maneira dinâmica você criar regras do *firewall*. Eu diria o seguinte: todas as ferramentas

complementares são úteis, tá, tudo o que você botar a mais aí certamente ajuda. Eu só não encararia isso como a sua principal forma de defesa, tá, pessoal? Eu diria assim: Tira desse modo senha *only*, tá, e todo o resto só está... Aí, depois, todo o resto você escolhe, se você tem familiaridade com essas ferramentas ou não, se faz sentido no seu ambiente ou não, tá? Tem gente perguntando de *Port Knocking*. Se quiser usar *Port Knocking* também, quer dizer, gerar tráfego em uma porta X, e aí você toma uma ação e levanta um *daemon*, ou muda uma regra de *firewall* em função disso, tudo isso são complementares e têm seu espaço, tá, pessoal, mas eu não faria isso aí antes do básico do básico, que é: cara, não use mais SSH com senha *only*, tá? Então, depois, todo o resto que você quiser fazer é lucro.

SRA. CRISTINE HOEPERS: Klaus, tem uma pergunta ali do pessoal, acho que ficou em dúvida sobre a ideia de par de chave, não é, que... o que vai em cada máquina. Está no chat aqui do--

SR. KLAUS STEDING-JESSEN: Ah, sim. Ah, tá. É, no servidor, pessoal, vai aquela segunda linha ali... vai o *authorized keys*, vai o pub, vai a porção pública, tá? Você vai dar um *copy-paste* ali da porção pública da chave e vai colocar no *authorized keys* do usuário que você quer se autenticar e 'logar' lá, tá? E a porção privada, tá, aquele primeiro arquivo, é que vai ficar no cliente, é quem está originando a conexão SSH, tá? Então, você precisa deste cara, tá, da porção privada para... no cliente e você precisa da porção pública no servidor, no *authorized keys* do usuário que você pretende conectar, tá? Quando eu falo conectar pode ser o própria SSH, mas pode ser SCP, quer dizer, qualquer coisa que use o protocolo SSH, tá? Eu acho que... Espero ter resolvido essa dúvida aí.

SRA. CRISTINE HOEPERS: Bom, pessoal, a gente... Como a gente está fazendo ao vivo e a gente queria poder ir pegando as perguntas, tal, a gente vai fazer, eu e o Klaus, uma pequena pausa, mas não a apresentação. Eu vou passar de novo... eu vou passar a palavra para o Eduardo, e, na volta, a gente vai falar de toda a parte de incidentes, a parte de como priorizar, detectar e, principalmente, de várias perguntas que o pessoal fez: Ah, como eu vejo se minha rede está gerando ataque, se não está? Como é que... impedir a parte de *netflow*, e a gente vai fazer isso daqui... entre cinco, dez minutinhos, mas eu vou passar para... vou parar o compartilhamento aqui. Não sei se o Klaus quer fazer alguma outra palavra, mas eu passo para o Eduardo já, e aí ele já assume aí.

SR. KLAUS STEDING-JESSEN: É, não, podemos passar para o Eduardo, sim. Eduardo, manda bala.

SR. EDUARDO BARASAL MORALES: Não, está certo. Pessoal, a aula de hoje, não é, ela não tem nenhuma parte gravada, então os

palestrantes, eles pediram essa pausa para ir no banheiro, mas a gente vai gerar aí alguns avisos para vocês, tá?

Então, lembrando do certificado, se você quiser o certificado desta live, as inscrições, elas vão até às 2h da tarde. O pessoal está colocando o link no chat do Youtube. Então, se inscreva, e, também, fique atento ao seu e-mail, porque vai um link de confirmação no seu e-mail. Clicou no link, aí você vai ganhar o certificado.

A questão, também, do formulário de avaliação. Então, como a gente sempre pede, a gente quer um feedback sobre o que você está achando dessa live. Então, o pessoal está colocando agora o QR Code aí na tela para vocês responderem. São duas perguntinhas simples, e o que a gente pede é que você dê uma nota de um até dez para essa live e escreva um comentário, se você está gostando ou não está gostando, o que a gente pode melhorar. Então, por favor, nos ajude, porque isso é muito importante, tá?

O Moreiras até fez uma brincadeirinha no começo da live falando ali do moletom do IX.br, mas eu queria lembrar que na feira virtual que a gente vai ter amanhã, às 2h da tarde, a gente vai ter um caça ao tesouro, e no caça ao tesouro vai ter uma camiseta polo da Semana de Capacitação do NIC.br. Essa é uma camiseta que a gente fez para distribuir nos eventos presenciais. Foi no começo da pandemia, a gente não conseguiu fazer nenhuma edição presencial, e elas estão todas guardadas aqui no nosso estoque, e a gente decidiu colocar como um brinde. Então, além das pessoas do NIC.br que têm essa camiseta, você vai ser a única pessoa de fora do NIC.br que vai poder ter essa camiseta aí da Semana de Capacitação. Claro, se você ganhar o caça ao tesouro.

Então, já falando um pouquinho da feira virtual amanhã, que vão ter sorteios, vão ter ali interações, você pode fazer *networking*, a gente vai ter esse caça ao tesouro, tá, que você vai poder buscar as pistas, a gente quer fazer um pouco ali de gamificação. Então, você busca as pistas, vai ter ali algumas dicas, e aí aquele que chegar em primeiro lugar no caça ao tesouro vai ganhar vários brindes, não é? Até vou comentar aqui: vai ter uma caneca da ICANN; um kit de acessórios para vinho da Cisco; uma caixinha de som a prova d'água da Cisco; um copo sustentável da Logicalis; um *voucher* da Globoplay de acesso para acesso para dois meses da Globo; um livro Vida de Programador, volume 0, da Novatec; um livro Vida de Programador, volume 1, da Novatec; uma camisa polo da Semana de Capacitação do NIC.br; uma lapiseira da Semana de Capacitação do NIC.br; um kit de adesivos individuais do IPv6 e do RPKI do NIC.br; uma garrafinha de alumínio e uma caneta personalizada da Juni Giovaneli; e um roteador Huawei Wi-Fi Mesh WS5800 da FiberX e Huawei. Então, é um caça ao tesouro mesmo, você vai achar ali um grande brinde, ali, se você ganhar, tá?

Agora, eu vou pedir para o pessoal colocar o videozinho da feira virtual. Então, pode tocar aí o videozinho, pessoal.

[exibição de vídeo]

SR. ANTONIO MARCOS MOREIRAS: Pessoal, vocês estão gostando da aula da Cristine e do Klaus até agora? Digam para a gente aí no chat, como é que está para vocês? Vocês estão apreciando, estão achando útil para o dia a dia? Eu acho que isso que é o mais importante, não é? Se vocês estão achando que isso vai ser algo útil ou algo que pode ser implantado, utilizado, as dicas, nos provedores de vocês até agora, se bem que até agora o pessoal falou bastante dos problemas em si, não é, mas já começaram também a dar algumas dicas úteis muito interessantes aí.

SR. EDUARDO BARASAL MORALES: Sim, Moreiras, teve até uma dica: é mais importante você ter mais segurança que o vizinho, tem que ter mais cadeado na sua casa do que na do vizinho, porque daí o atacante vai para a casa do vizinho.

[risos]

SR. ANTONIO MARCOS MOREIRAS: É uma dica excelente, não é, Eduardo? Muito boa mesmo. Muito legal, gente, vocês estão achando isso. Olha, então, fica uma outra dica para vocês aqui: quando acabar essa aula, quando acabar o dia de hoje, manda esse videozinho, manda o link do vídeo, que ele vai ficar gravado no Youtube, manda para os colegas, não é, manda para o pessoal, porque, cara, esse vídeo aqui é o tipo do vídeo que devia viralizar. Apesar de ser um vídeo de três horas, não é, porque não acabou ainda, daqui a pouco a Cristine e o Klaus voltam, é um vídeo que tem um conteúdo muito, muito importante para o pessoal dos provedores. Essa questão de segurança é uma questão fundamental.

Estou vendo aqui que tem 750 pessoas assistindo agora aqui, ao vivo, com a gente, presentes, e só temos 490 *likes*, não é? Muito pouquinho esses *likes*. Como eu falei no começo do vídeo, gente, é importante para a gente que vocês deem o *like,* porque isso incentiva o YouTube, incentiva o Facebook, para quem está acompanhando no Facebook, a distribuir esse vídeo, a mostrar esse vídeo para mais gente aí. Como eu disse, o conteúdo é extremamente importante. Essa aula da Cristine e do Klaus é uma aula extremamente rica, não é, cheia de dicas e de conhecimento que dificilmente vocês vão achar em um curso por aí e que são importantes para o negócio de vocês, são importantes para a boa operação do provedor de vocês, da rede de vocês. Então, é um conteúdo que, primeiro, merece um *like*, não é? Cá entre nós, merece um *like*. Não é porque é da gente aqui do NIC.br, mas é um conteúdo, modéstia à parte, pela Cris e pelo Klaus, que não sou eu que

estou falando, não é o Eduardo que está falando, não é, mas, modéstia à parte, pelo NIC.br é um conteúdo muito bom. Você há de convir. Vocês mesmo disseram, perguntei antes de falar isso, não é, vocês mesmo concordaram que é um conteúdo muito bom. E também ajuda na distribuição disso para mais gente.

Temos um *dislike* também. Eu lembro de uma live em que eu disse para o pessoal que se não gostasse podia dar *dislike*. Desde então, em toda live a gente tem um *dislike*. Está lá sempre, a pessoa entra no começo da live, dá o *dislike* e fica lá registrado, mas também é um direito de vocês. Quem não gostar ou não concordar, dá o *dislike*, não é? Passa aí.

Gente, o moletom. Eu fiquei com peso na consciência aqui, porque eu fiz uma brincadeira no começo da live e tem gente que leva as brincadeiras muito literalmente, não é? Eu vi uns comentários no chat aí de gente que... eu não sei se estava brincando também ou se não entendeu a brincadeira, então deixa eu falar claramente. Esse moletom aqui, esse tipo de moletom aqui, com o IX.br, com essa touquinha aqui bem chamativa, aqui, com essa cor legal, esse é só para funcionários, não é? Então, a brincadeira que eu fiz foi dizer que a gente tem algumas vagas abertas, inclusive no IX.br, e que essas vagas ficam publicadas lá no site do NIC.br, que se você quer tanto um moletom assim, olha a vaga e vem trabalhar com a gente. Mas o moletom é só para funcionários. Agora, como o Eduardo falou, existem outras coisas aí, por exemplo, a própria camisa polo da Semana de Capacitação, que vai estar como prêmio lá na feira.

E falando da feira, vamos aqui, enquanto a Cristine e o Klaus tomam aquela água, não é, vão no banheiro... quem quiser, também, aproveita aí para dar aquela corridinha e tomar um copo d'água, ir no banheiro. Daqui a pouco, a Cristine e o Klaus estão aqui conversando com vocês de novo, mas enquanto isso, vamos dar uma olhadinha em um ou outro detalhe da plataforma onde amanhã a gente vai fazer a feira virtual, não é, que é a Gather Town. Vocês devem já estar vendo aí na tela de vocês eu e o Eduardo aqui na plataforma Gather Town. Não é exatamente essa a cara que vocês vão ver amanhã na feira virtual. A gente mandou fazer... Essa é, vamos dizer assim, é como se fosse uma tela de demonstração da plataforma, e a gente mandou fazer um fundo todo diferente, todo... com um mundo de redes de Telecom, de Internet, não é, referenciando coisas legais, e com essa cara também de game 2D, e eu acho que vocês vão gostar. A gente preparou aí um cenário, vamos dizer assim, todo especial para essa feira, para vocês. Bom, gente, daí essa plataforma, para quem não viu a demonstração, não conseguiu pegar a ideia no vídeo, ela permite interações muito semelhantes às que a gente teria em uma feira real, não é, em uma feira presencial. Real não, não é, porque essa vai ser bem real. Apesar de ser... a gente estar remoto, a gente estar

virtualmente em um ambiente, as interações com as pessoas são reais, e a gente quer, justamente, deixar elas possíveis e mais reais que a gente conseguir. Então, olha, vê, eu vou me afastar do Eduardo aqui, olha, a câmera dele some na tela. Se eu voltar e encontrar ele, olha, a câmera aparece. A gente poderia estar conversando aqui por voz e vídeo, não é? A gente não está fazendo isso agora, porque senão vai dar uma microfonia danada na transmissão aqui do YouTube. Vejam também que tem... Quando eu me aproximo dessa lousa, ela fica amarelinha. Tem alguns objetos que a gente pode interagir, então, podem ser mensagens, podem ser vídeos. Apareceu aqui na minha tela "pressione o X do seu teclado para ver o conteúdo". Vou fazer isso agora. Isso é só para demonstração. Eu pressionei o X. Está demorando um pouquinho para carregar aqui, porque eu estou na Internet de casa, ela não é tão rápida, mas é aqui.

SR. EDUARDO BARASAL MORALES: Moreiras.

SR. ANTONIO MARCOS MOREIRAS: Fala, Eduardo.

SR. EDUARDO BARASAL MORALES: Também é legal de comentar que... como anda, não é, na plataforma, não é? Tem que usar as setinhas para você mexer o seu avatar. Parece intuitivo, mas muitas pessoas vão ficar perdidas, não é?

SR. ANTONIO MARCOS MOREIRAS: Ah, é verdade.

SR. EDUARDO BARASAL MORALES: Então, além do X, tem que usar as setinhas.

SR. ANTONIO MARCOS MOREIRAS: As setinhas do teclado, normais, como se você estivesse em um *game*, não é? Aquelas setinhas, você consegue andar.

Então, agora, vamos supor que o Eduardo está longe. Eduardo, vai embora aí, vai para longe de mim. O Eduardo foi para longe aí. Vamos supor que o Eduardo não é o Eduardo, o Eduardo é o Eduardo da empresa Acme Tecnologia, e eu estou muito interessado em falar com o Eduardo da Acme Tecnologia na feira. O que eu vou fazer? Eu vou vir aqui nessa relação de participantes. Poxa, mas aqui eu estou vendo o Eduardo. Obviamente, amanhã, cara, vai ter 500 pessoas na feira, literalmente, esperamos, e eu não vou conseguir achar o Eduardo aqui na lista. Então, o que eu vou fazer? Eu vou fazer uma busca. E a gente vai pedir para todo mundo, é claro que dá para entrar de uma forma diferente, mas a gente vai pedir para todo mundo que entrar na plataforma, entrar dessa forma, colocar o nome e, entre parêntese, a empresa. E os palestrantes da Semana de Capacitação vão estar com o nome identificado também, com o conteúdo que ele deu na semana de capacitação, o nome dele e a empresa. Então, você vai poder fazer busca tanto pelo nome do palestrante em si ou pelo nome do participante, do visitante da feira, como pela empresa dele. Ah, eu

quero falar com alguém do Netflix, não é? Você vai procurar aqui "Netflix" e vai conseguir achar o pessoal, que vai, inclusive, estar amanhã aqui palestrando também e vai estar na feira. Você quer achar alguém da Globo, não é, para falar sobre CDN, alguma coisa? Vai estar aqui. Quer achar os palestrantes de segunda-feira, de terça-feira, vai procurar por aqui. Daí eu quero achar o Eduardo agora. Eu tenho duas opções aqui, não é? Eu posso clicar aqui com o botão direito e dar um *follow* no Eduardo, eu mando seguir o Eduardo, o meu avatar aqui, ele vai automaticamente atrás do Eduardo; ou eu posso dar um "*locate on map*", e daí vai aparecer o caminho para eu chegar até o Eduardo, olha. Eu mandei localizar. Olha, apareceu um caminho aqui, eu vou... eu estou seguindo manualmente esse caminho, eu optei por essa segunda opção. Olha aqui, e está aqui o Eduardo, achei o Eduardo.

SR. EDUARDO BARASAL MORALES: Moreiras, acho que também é legal a gente ter... de comentar que vai ter o pessoal, também, do Intra Rede, não é, do Camada8. A gente está convidando os palestrantes das lives passadas para estarem dentro da plataforma. Então, ficou uma dúvida de alguma live do Intra Rede, quer ali conversar com o palestrante? Tem a oportunidade de ir lá no estande do Intra Rede, do Camada8, e conversar com ele, se ele tiver ali na plataforma. E temos, também, ali poucas vagas, não é? Você falou 500, mas 500 é o nosso limite aí dentro da plataforma. Então, pessoal, não percam tempo. Na hora que a gente liberar a plataforma, já entra, porque a gente tem ali 500 pessoas no total, ali, do pico, não é? As pessoas podem--

SR. ANTONIO MARCOS MOREIRAS: Exatamente.

SR. EDUARDO BARASAL MORALES: Sair, entrar, sair, mas é 500 no total em pico.

SR. ANTONIO MARCOS MOREIRAS: O limite dessa plataforma são 500 pessoas simultâneas, não é? Então, não percam tempo mesmo, porque--

SR. EDUARDO BARASAL MORALES: Fica na fila de espera.

SR. ANTONIO MARCOS MOREIRAS: Se deu 500 pessoas o sistema não vai aceitar a conexão. Aí você vai tentar um pouquinho mais tarde, não é? Esperar alguém sair, não é? É isso, não é, Eduardo? Para evitar aglomeração, não é?

[risos]

SR. EDUARDO BARASAL MORALES: É, exatamente. E aí... É, estamos na pandemia, não pode ter muita gente junto, não é? E é exatamente o que você falou, Moreiras, se você não conseguiu entrar porque deu ali o limite de 500 pessoas, o que a gente fala? Espera ali uns 15 minutinhos, dá ali uns 20 minutos, tenta de novo, tá, porque é o limite da plataforma, não é? Como a gente está com 700 pessoas, se

todo mundo quiser, 200 vão ficar para fora, mas nem todo mundo vai ficar as duas horas. Então, tenta entrar um pouquinho mais tarde para poder conversar, interagir, tudo, mas lembra: a gente vai estar com o caça ao tesouro rolando. Então, quem quiser ali ganhar todos aqueles prêmios ou participar do *game* tem que entrar logo que a gente abrir a plataforma, não é?

SR. ANTONIO MARCOS MOREIRAS: É. E o pessoal do NIC também vai estar lá, pelo menos o pessoal da nossa equipe, não é, Eduardo? Nós vamos estar na feira lá para conversar com vocês. O pessoal da engenharia do IX.br já confirmou com a gente também que vai sempre ter gente lá no estande do NIC.br para conversar com vocês. Então, também é uma oportunidade para conversar com os próprios funcionários do NIC.br, se vocês quiserem e quiserem... de algumas áreas. Por exemplo, o pessoal do PTT, não é, e o pessoal da nossa equipe vai estar lá presente com certeza para tirar as dúvidas de vocês e bater um papo com vocês aí durante a feira. E acho que é isso, não é? Tem mais alguma coisa que você queira mostrar aí, Eduardo? Já vimos aí que a Cristine e o Klaus já estão aqui preparados para voltar. Tem mais algo--

SR. EDUARDO BARASAL MORALES: Eu acho que pode voltar para a aula, não é? Dar um tempo a mais aí para o pessoal tirar as dúvidas da área de segurança. Então, escrevam, pessoal, no chat, as perguntas aí para o Klaus, para a Cris, que vocês queiram tirar de dúvidas. Então, esse é o momento. Eu acho que podia voltar para a aula.

SR. ANTONIO MARCOS MOREIRAS: Então, é isso aí, gente. Vamos voltar agora para a Cristine e para o Klaus. Eu passo a palavra, e boa continuação de aula para vocês.

SRA. CRISTINE HOEPERS: Perfeito, Moreiras. Eu vou aqui colocando, acho que o Klaus podia ir tirando uma dúvida que a gente viu ali no chat que a gente achou que é pertinente, enquanto eu compartilho aqui.

SR. KLAUS STEDING-JESSEN: Era uma dúvida, pessoal, falando sobre... Tá, mas como é que é esse gerenciamento de chaves, não é, SSH em um ambiente onde tem múltiplas pessoas usando? E a ideia aqui, pessoal, é um par de chaves por pessoa, tá? Então, só para deixar claro isso, assim, cada um tem a sua chave, cada um cuida da sua... desse par, e você, então, vai colocando nos *authorized keys* as chaves de cada uma dessas pessoas aí. Só para deixar claro que isso aí é individual, tá, pessoal? Não estamos falando de compartilhamento de um par de chaves para N pessoas da organização, tá? Eu acho que era mais ou menos por aí, não é, Cris?

SRA. CRISTINE HOEPERS: É, acho que era. Acho que a dúvida também é se é uma mesma conta que tem que acessar, se dava até mais de uma chave para uma mesma conta, por exemplo.

SR. KLAUS STEDING-JESSEN: Sim, sem problema. Você põe... em um mesmo *authorized keys* da conta *root*, por exemplo, você põe N chaves. Cada pessoa tem a sua e cada um vai entrar aí no... E você consegue ver quem entrou, não é, porque pelos *Logs* você vai ver que chave que foi usada na hora. O servidor SSH, ele vai 'logar' isso daí. Então, isso aí é tranquilo também.

Eu acho que a gente podia avançar, pessoal, naquele quesito em que a sua organização, o seu provedor, o seu AS vai receber notificações de terceiros. Então, para facilitar a vida de vocês, como é que são esses e-mails do CERT, tá? Então, assim, a gente... O e-mail é bem-comportado, tá? Os cabeçalhos, se você quiser filtrar, você vai ver que vai vir de um "*from*: cert@cert.br". O *envelop from*, não é, o *return-path* vai ser ali um cert@cert.br também. O e-mail sempre é entregue por um mesmo servidor nosso, tá, esse servidor que vocês estão vendo aí, woq.cert.br. Nesse caso, v6, mas tem v4 também, não é? E sempre vai estar assinado com DKIM, tá? Então, para quem checa as assinaturas DKIM, aí você vai ver que vai vir assinado direitinho, tá? Então, uma sugestão que a gente tem é: priorizem esses e-mails. Primeira coisa, agora, pessoal, enquanto vocês estão nos assistindo, é: primeira coisa, faz um Whois para um IP seu, um AS seu, e vê o que aparece no Whois como seu *abuse contact*, quem estaria recebendo esse e-mail. Primeira coisa é consertar isso se não estiver certo. "Ah, mas está indo para o consultor que não lê os meus e-mails", tal. Hora de mudar isso aí, tá? "Ah, mas cai em uma caixa que, putz, a gente só... não achava que vinha nada relevante", tá? Então, mudem isso, tá, e tentem priorizar. Eu acho que vai ser, como a gente comentou aqui, um mecanismo... Cara, não custa nada, tá? A gente tem um grande esforço aqui no CERT para mandar coisas relevantes, tá? A gente não fica mandando coisa errada, tá, ou a qualquer hora. A gente só manda coisas que a gente sente que é realmente importante. Então, mais um motivo aí para vocês priorizarem essas notificações, tá?

SRA. CRISTINE HOEPERS: Pois é. Até colocando acho que em cima disso aqui aquele comentário que eu fiz antes, não é? As mensagens que a gente manda vão ter dicas. Então, tentem fazer qualquer maneira, não é, seja uma regra de *spam*, um *procmail*, chegou, vai para um outro *folder*, não é? Tentem colocar essa parte. Klaus, teve uma pergunta muito interessante, que, na verdade, já foi respondida no chat, mas eu vou colocar aqui, de SSH, que o pessoal falou: "Ah, mas e se daí o colaborador sai do provedor, o que eu faço?". E a resposta foi o que o pessoal botou... Aí você resolve tirando a chave do colaborador--

SR. KLAUS STEDING-JESSEN: Do *authorized*--

SRA. CRISTINE HOEPERS: Do *authorized keys*.

SR. KLAUS STEDING-JESSEN: Exatamente. Exatamente.

SRA. CRISTINE HOEPERS: Entendeu? Então, assim, é isso aí. E fica mais fácil de controlar, porque não é uma senha compartilhada, é uma chave, a *passphrase* é aquela *passphrase* que a pessoa colocou naquela chave dela, e se aquela chave estiver em múltiplos servidores, o pessoal até falou: "Ah, dá para automatizar com Puppet, com Ansible, com alguma coisa", mas é uma maneira, inclusive, de rapidamente você tirar acesso se uma chave for comprometida. Você vai lá e tira do *authorized keys*, não é?

SR. KLAUS STEDING-JESSEN: E essa dica, Cris, de Ansible e... ou seja qualquer coisa que automatize, isso aí eu acho que é muito valiosa, tá, porque a gente ouve muitas vezes assim: "Ah, não, isso aí é muito bonito, mas eu tenho, cara, que gerenciar 500 servidores em um *Data Center*", tá? Mais um motivo para você pensar em um esquema que você automatiza, não é, tem N soluções por aí, e aí de um local você faz isso. Um clique, um *Enter* seu, faz isso em 500 servidores, tá, e rapidamente você revogou, por exemplo, aquela credencial, tá? Então, eu acho que é uma boa discussão, assim.

Pessoal, só... E aí? Exemplos de uma mensagem do CERT.br, tá? Esse é um exemplo real, tá? A gente só [ininteligível], obviamente, ali os IPs e AS, que a gente notificou há poucos dias de amplificação *Portmap*. Podia ser qualquer outra coisa, tá? Então, em geral, vai ter esse jeitão aí, como eu falei, esses *headers* que a gente comentou, vai ter um texto dizendo, sim, o que a gente está solicitando, tá, *Logs*, naquele caso ali embaixo vão ter *timestamps* que a gente testou, tá, esse formato ISO de data, e resultado do teste. Nesse caso, está dizendo que aquele IP que não aparece aí, está [ininteligível], não é, ele é *open* para *Portmap*. Nesses casos, a gente, inclusive, bota mais detalhes de quantos bytes o negócio respondeu, etc. e tal. E, em geral, assim, a gente tenta sempre colocar nesse jeitão, logo de cara o que estamos pedindo e qual é o *Log*, tá, e depois, a gente vai colocar um negócio um pouco mais verboso, tá, do tipo: Tá, mas e aí, o que eu faço? Onde é que eu obtenho mais informações, etc. e tal? Tá? Então, esse é um jeitão clássico de um e-mail nosso, então, para o pessoal. Eu tenho certeza que quem está nos assistindo aqui já deve ter recebido alguma coisa de algum... alguma notificação nesse sentido, tá? E como eu falei, eu acho que a gente tem que... Encarem, pessoal, não é um CERT... "Ah, meu Deus, o CERT está me vigiando". A gente está querendo ajudar o nosso ecossistema aqui do BR. Então, encarem isso como um alerta para ajudar o seu provedor, ajudar a Internet, não é, porque a gente tem esse dado na mão, a gente se sente na obrigação de compartilhar com vocês, tá? Ninguém está aqui obrigando

ninguém a fazer nada, tá, não é o nosso papel. O nosso papel é subir a barra da segurança nas nossas redes aqui no Brasil. Assim, é simples assim, tá? Ninguém está aqui julgando ninguém. "Ah, não, mas, putz, recebi essa notificação". Que bom que você recebeu e que você é o dono do ativo e você pode ir lá resolver, tá? É simples assim, tá? Não sei se você quer complementar aí, Cris.

SRA. CRISTINE HOEPERS: Não, é bem por aí. E lembrar... Assim, claro, aqui a gente não botou tudo, não é, mas o próprio texto fala: Aqui abaixo tem mais detalhes do porquê que está recebendo e como resolver o problema", tá? Então, assim, a gente tenta sempre, ao máximo possível, colocar comandos ou colocar um link, por exemplo, para um documento onde tem um passo a passo de como resolver o problema. Às vezes é um documento do próprio fabricante, às vezes é alguém que tem uma... essa informação, não é? Então, como o Klaus falou, o nosso objetivo é ajudar as redes identificando especificamente qual é o problema e já com uma sugestão de como resolver. Claro que cada rede é específica. Pode ser que você está usando alguma ferramenta especial, pode ser que você tenha uma ferramenta que automatize ou não automatize. A gente sempre vai tentar colocar a maneira mais simples de resolver o problema. Mas se vocês puderem tentar olhar lá nos e-mails de vocês... A gente colocou essas dicas aqui para priorizar, porque é, sim, muito comum, não é? A nossa equipe que lida com tratamento de incidentes, que não é diretamente eu e o Klaus, não é, vocês interagem muito com o Renato, com o Cordeiro, com o Chico, que são... que é quem está no dia a dia fazendo ali a rotação de triagem, e às vezes entra em contato, liga lá e vocês: "Ah, perdi o e-mail, não vi, como é que eu faço para achar?". Então, assim, a gente está mandando informações que são para ajudar vocês, e para ajudar vocês a ver problemas bem específicos e já com uma dica de como corrigir esse problema, não é? Então, esse é o nosso intuito mesmo quando a gente manda essas notificações aí.

SR. KLAUS STEDING-JESSEN: Perfeito, Cris. Acho que a gente podia, então, avançar um pouquinho, entrar nessa parte de *netflows*, não é, que é algo que a gente já tinha prometido. Só um preâmbulo aqui, pessoal. Quando a gente está falando de... Bom, primeiro, quando a gente está falando de *netflow*, é algo que, em geral, já está disponível nos seus elementos de rede, tá, às vezes pode não ter exatamente esse nome, pode ser sFlow, Netflow, IPFIX, etc., tá? Em geral, ele já está disponível, tem custo zero, tá? O software que faz, depois a gente vai mostrar a topologia ali, mas o software que faz a coleta pode ser feito com um software livre, tá, custo zero, tá bom? E o que a gente está querendo reforçar, não é? Aquela questão de telemetria, vamos dizer, de entender, de saber o que está acontecendo na sua rede, tá? Muitas vezes, a gente escuta assim de provedores: "Ah, sim, sim, nós já temos *netflow*, mas é usado só para engenheira

de tráfego. Eu quero saber com que protocolos ou que volume de dados eu troco com os meus diferentes ASs aí que eu faço os meus trânsitos, etc.", tá? Sim, certamente dá para fazer para isso, mas o que a gente queria reforçar aqui para vocês, pessoal, é que sim, tem um uso muito interessante de *netflow* para segurança, tá? Alguns exemplos aqui. Depois, a gente vai mostrar uns exemplos mais específicos, mas, por exemplo, detecção de *botnet*, tá? Eu quero saber que IPs da minha rede estão falando com comando e controle conhecidos, tá? A gente vai ver que tem como obter essas informações de maneira gratuita, tá? Eu quero saber DDoS saindo da sua rede, tá, volume, etc., tá? Outra coisa muito, muito útil: dado histórico para investigação de incidentes, tá? Imagina que você tem o seu *netflow* sendo guardado por uma janela aí de X meses, tá, você descobriu que uma determinada máquina da sua rede, um servidor seu foi invadido em coisa de X tempo atrás, você poder "voltar no tempo", voltar no seu *netflow* e começar a descobrir: "Vem cá, mas quando é que essa máquina começou a originar determinado tipo de tráfego?". Ah, foi no dia tal. "Ah, tá, mas antes disso aconteceu o quê?". Putz, aconteceu uma conexão vindo da rede Y, não é? E você ir reconstruindo esse incidente é muito valioso, pessoal, e assim... E para isso funcionar, obviamente, você já tem que estar tendo isso em produção antes do incidente, não é? A gente vê muitos casos em que a pessoa tenta: "Não, não, agora eu vou ligar *netflow* para ver o que eu consigo descobrir". Bom, aí é muito tarde, não é? Quer dizer, o negócio já se arrastava há meses, esse incidente, tá? Então, isso é algo que pode ser muito, muito útil, tá, nesses casos aí de dado histórico de investigação de incidentes, tá?

SRA. CRISTINE HOEPERS: Klaus, até antes de começar a explicar *flow*, duas coisas que meio que me vieram à mente aqui. Um, pessoal, que, assim, não acreditem no mito do: "Ah, eu não consigo capturar 100% logo, então não adianta". Sempre adianta. Não tem problema quando é... Capturem, sei lá, 1 para 10 mil, 1 para mil, um para... A gente tem casos de 1 para 32 mil pacotes, mas coletem alguma coisa. Talvez, façam algo diferente, 1 para a rede do *backbone* inteiro, e pensem em um 'netflowzinho', assim, para a rede principal lá de vocês, não é? Hoje em dia, com esses tempos de LGPD, não é, onde que fica a rede de vocês, onde estão todos os dados de clientes, onde vocês fazem as coisas de pagamento. Quer dizer, como é que fica essa parte também de incidentes e de identificar comprometimentos da infraestrutura de vocês, e não só *botnets* e DDoS saindo, por exemplo, da rede de clientes, não é? Então, pensem que vocês podem ter níveis diferentes de captura de *netflow* dependendo do uso que vocês queiram dar para isso, tá? Então, assim, um que sempre é importante, o outro para investigação de incidente é extremamente valioso. E aí, vocês podem também querer ter tempos diferentes de guardar essa informação, não é? Então, pensem aí que vocês podem ter múltiplos pontos capturando os *flows* na rede de vocês.

SR. KLAUS STEDING-JESSEN: E essa dica é importante, viu, Cris, porque, às vezes, a gente escuta de provedor assim: "Ah, mas eu tenho uma caixa X que eu já tentei fazer 1 para 1 e ela não aguenta", não é? Mais um motivo, então, para você usar *sampling*, tá? Assim, ache um *sampling* que faz sentido para o seu volume de tráfego e para o *hardware* que você tem, tá, mas não caia nessa do: "Ah, não, mas, putz, já que não é 1 para 1, logo não serve para nada", tá? A gente tem, como a Cris falou, vários casos de... Bom, algumas tecnologias, inclusive, você é obrigado a usar *sampling*, tá, 1 para 512, etc., e ambientes de muito tráfego, e estamos falando de coisas de X da vida, bom, aí nós estamos falando de 1 para 30 mil, sabe? Coisas, assim, realmente... E ainda assim são valiosas, tá? Você consegue ver tráfego malicioso, e como a gente falou, você quer ver, você quer ter respondidas perguntas do tipo: "Quem está falando com um determinado comando e controle? Quem está falando com um DNS malicioso e que eu sei que é malicioso?", tá, de maneira que você consegue, então, limpar a sua rede, tá? A ideia toda aqui, pessoal, é te dar uma ferramenta que você possa ir atrás dos problemas e limpar a rede, tá? Essa que eu acho que seria a ideia aí, tá?

Então, só para a gente relembrar, pessoal, o que estamos falando de *netflow*? A gente vê nos nossos cursos uma confusão grande, tá, pessoal, porque muitas vezes, quando o pessoal... o pessoal meio que abrevia isso para *flow*, tá? "Ah, eu tenho *flow*", "eu capturo *flow*", não é? E, infelizmente, cada um interpreta de uma maneira. O que é *flow*? Tem gente que diz: Ah, sim, sim, eu faço... eu espelho aqui, uma porta do meu *Switch* e capturo tudo com tcpdump". Não, não é isso que estamos falando, tá, pessoal? Por *netflow* a gente está falando de tecnologias... e começou lá atrás com Cisco, hoje é um padrão IETF, tá, IPFIX, mas são todas essas tecnologias de, vamos dizer, de sumarização de tráfego, tá? Então, assim, por exemplo, neste exemplo simples aqui, imagina que eu tenho um cliente falando com um *server*, tá, um servidor, porta 80 TCP ali, tá? Então, qual é a ideia? Eu tenho um elemento no meio do caminho aqui, um *Switch*, um *Router*, pode ser... hoje em dia tem *firewall* que gera *flow*, tem N maneiras, tá? Então, esse camarada no meio do caminho, ele vai, então, exportar esses *flows*. Imaginem, encarem eles como um registro de tudo o que está passando por ele. Mas eu não vou 'logar' pacote a pacote, tá? Ele vai me 'logar' mais alto nível isso. Então, esse registro do que está acontecendo, ele basicamente vai falar o seguinte: "Olha, eu observei um IP de origem X falando com um IP de destino Y na porta de origem, porta de destino tal, no protocolo tal", tá? Isso aqui é bem simplificado, pessoal, pode ter N outras coisas, tá? Posso ter AS de origem, AS de destino, posso ter... certamente, eu vou ter duração que essa comunicação se deu, volume de pacotes, volume de bytes, etc. e tal. E isso, então, é exportado, tá, para um coletor de *flows*. Como a gente comentou antes, isso pode ser simples, como nfdump e nfcapd. São

ferramentas de código aberto, tá, funcionam muito bem. Tem soluções pagas também, tem N opções, tá? Mas a ideia é que isso vá para um coletor seu, ser guardado em disco, você que vai ter que determinar quanto disco você tem, qual o seu volume de rede e por quanto tempo você precisa disso, e a ideia é que você vá fazer consultas para cima desses dados coletados, tá? Então, aí que mora a utilidade desse modelo, tá? [Então, se você quiser avançar aí, Cris.]

Então, basicamente, essa--

SRA. CRISTINE HOEPERS: Klaus, você estava... Só para te falar, você estava falando de ferramenta, não é, e de novo aquilo que você comentou, tinha um pessoal perguntando: "Ah, Wireshark é *flow*?", tal. Não, Wireshark é o que está passando no fio, Wireshark é tcpdump, ele vai pegar--

SR. KLAUS STEDING-JESSEN: É, exatamente.

SRA. CRISTINE HOEPERS: Todo o conteúdo e você vai ter o pacote inteiro. O *flow*, ele é só um sumariozinho, é como se você tivesse um guarda de trânsito anotando a placa dos carros passando no cruzamento. Você vai ter aqui alguém que vai ver pacote e falou: IP tal, IP tal, porta, porta, TCP tal, passou. Você não tem conteúdo, tá? Você tem só, realmente, esse sumário, e geralmente tem número de bytes que passaram, você consegue ter, por exemplo... não é pacote a pacote. Você começou: "Hum, tá". Passou... começou essa sessão aqui, o cliente [ininteligível] com o servidor na porta 80, quando ela termina, não é, quando tem o fim e terminou a conexão, ele vai dizer: Ah, sim, começou tal hora, terminou tal hora e passou tantos bytes, não é? Isso é só o sumário mesmo, é o resumão.

E ferramentas de software livre, que o pessoal estava perguntando também, nfcapd, nfdump, a gente... No final dessa sessão, tem links para o site do nfdump, mas até uma coisa que eu ia dizer assim, o pessoal ali falou muito: "Ah, tem ferramentas para ver *flows*", não é? Para segurança, para a gente não interessa muito ficar vendo volume de tráfego, tal. Pode até ser que você tenha algo aparecendo ali naquelas ferramentas gráficas, tal, mas o que a gente vai querer fazer são consultas, não é, são coisas bem específicas procurando por determinados padrões de ataque, não é? Então, só vendo, assim, algumas discussões e perguntas ali, eu achei que seria legal a gente deixar isso bem claro, que Wireshark, tcpdump, está pegando tudo, o conteúdo inclusive, não é? Você até poderia usar o que sai do Wireshark, passar por um software que gerasse um *flow* a partir disso. Isso é possível fazer, não é? Mas, hoje em dia, o ideal seria você ter, até pelo volume de tráfego que a gente está falando, é ter o equipamento de rede que consiga exportar esses *flows* de uma maneira mais rápida aí para um coletor.

SR. KLAUS STEDING-JESSEN: E só complementando, Cris, não tirando o valor de Wireshark, tcpdump, etc. É óbvio que você ter *payload* pode ser muito interessante, mas lembrando, pessoal, que se você está rodando isso aqui em uma rede de produção, em um grande provedor, bom, não escala você ter *payload* de tudo, não é? Imagina equipamentos grandes, interface 10 gigas, não é, 100 gigas, etc., e você vai pacote a pacote guardar isso em um canto, não é? Então, aí que entra o poder das ferramentas, você... Como você está guardando só, vamos dizer, uma sumarização do que está passando, não é, esse resumo do que está passando, muita gente acha que isso não é útil para nada, mas a gente vai mostrar algumas consultas onde você pode descobrir bastante coisa só vendo esse resumo, não é, e com a vantagem que você não está entrando nos detalhes de *payload*, pessoal, tá? Então, aquela questão de: "Não, mas e como é que fica a privacidade dos meus usuários?". Não, eu não estou olhando *payload*, tá? Eu quero saber que protocolo que é, com quem está falando, tá? E isso é extremamente valioso. E, de novo, pessoal, a gente tem que sempre lembrar que você está usando isso com um objetivo, que é aumentar a segurança da sua rede e saber o que está acontecendo na sua rede. Ninguém está fazendo isso aqui para monitorar usuário A, B ou C, não é?

SRA. CRISTINE HOEPERS: É.

SR. KLAUS STEDING-JESSEN: Então, eu acho que isso tem que ficar bem claro também, não é?

SRA. CRISTINE HOEPERS: Klaus, e dadas algumas dúvidas também que tiveram, o *netflow* é exatamente você não precisar fazer TAP de rede, não é? Porque eles perguntaram: "Ah, seria como um TAP?". Não, essa não é a ideia. Pode até ser que você queira fazer um TAP, daí coletar o *flow* lá e tal, mas a ideia do *flow* é você não fazer uma cópia do tráfego todo, é você ter algum elemento seu que vai exportando. E sim, dá para exportar de Linux, não é? Tem... acho que no final a gente até tem links que comentam disso. Você, na verdade, tem ferramentas que pegam... Você pode rodar em um *firewall*. A gente, por exemplo, gera *flows* nos nossos OpenBSDs, que são... o *firewall* de OpenBSD dos nossos *honeypots* gera *flows* dos *honeypots*, é gerado direto do *firewall* do próprio servidor ali, do próprio cliente *honeypot*, não é? E o pessoal também perguntou, Klaus, a diferença de sFlow e *netflow*. Talvez, se você pudesse complementar um pouco mais essa parte de nomenclatura que você citou rapidamente, mas só para deixar mais claro.

SR. KLAUS STEDING-JESSEN: É, ambos são exemplos de, vamos dizer, "*netflow* da categoria", não é? São só exemplos de diferentes fabricantes. O primeiro que a Cisco fez,chamou de *netflow*, tá? Então, assim, basicamente são variantes, tá, pessoal? Cada

fabricante, muitas vezes, dá uma... muda um pouco o nome e impõe algumas limitações. Por exemplo, de sFlow, se não me falha a memória, obrigatoriamente tem que ser 1 para 512 ou mais de *sampling*, tá? E aí, vai... Então, assim, a minha sugestão é: olhe o seu fabricante e vê o que ele tem, como é que ele chama essa tecnologia, tá? Como eu falei, o padrão IETF chama IPFIX, tá? Cada uma dessas tecnologias também tem versões diferentes, tá? Então, *netflow* V5, V7, V9. Então, algumas... Então, a primeira coisa que você precisa ver é o que o seu equipamento suporta, se nós estamos falando de um elemento de rede, tá? Isso pode, por exemplo, influenciar versões bem lá no começo, versão... o *netflow* V5, por exemplo, não suportava IPv6, tá? Depois, isso foi sendo colocado. Então, sugestão: vê o que você tem de equipamento e vê exatamente o que ele suporta, tá?

SRA. CRISTINE HOEPERS: E, Klaus--

SR. KLAUS STEDING-JESSEN: Como a Cris falou, vários *appliances* hoje fazem isso, *firewalls* fazem isso, tá? Então, não necessariamente você vai querer fazer isso... você é obrigado a fazer isso em um elemento de rede. Em geral, é a solução mais simples, tá? Simplesmente liga isso no seu *Switch* ou roteador e você tem isso daí. Pode falar, Cris.

SRA. CRISTINE HOEPERS: Klaus, o que eu ia comentar é que acho que a maioria das perguntas que estão vindo agora vão ser esclarecidas durante os exemplos, não é? E aí, talvez, só antes da gente entrar no exemplo, comentar que todos esses exemplos que a gente tem aqui, eles são... vão ser consultas que foram feitas via... a gente usando... eles foram conectados com... eram sFlow e a gente usou o nfcapd... O coletor era o nfcapd, não é, e a gente usou nfdump para consultar, tá? Então, só para vocês terem uma noção, assim, que nesse caso já era *sampling*, e aí as perguntas eram se dava para ver pacotes, bytes, como é que é, e eu acho que isso vai ficar tudo claro nos exemplos que a gente vai mostrar de consultas e o que a gente quer ver de segurança nessas consultas aí.

SR. KLAUS STEDING-JESSEN: Perfeito, perfeito. Eu acho que se o pessoal guardar essa parte aqui... Olha só, eu preciso de um elemento que exporte *flows*, tá? Então, por isso que a gente botou ali um "*Netflow-enabled*", nesse caso *Router*, mas pode ser um elemento de rede qualquer que consiga exportar os *flows*, ele vai exportar para alguém; esse alguém precisa coletar isso, tá? Então, em geral, é uma porta UDP configurável, e isso vai acabar se refletindo em um arquivo no seu *file system*, tá? Então, dependendo do software que você usar, isso é ordenado por data, tá? Então, assim, isso vai estar em um servidor seu, pode ser um servidor seu Linux, pode ser uma VM, tá, e isso vai acabar em disco. Uma vez que isso esteja em disco, você, então, daí consegue fazer consultas, tá? Então, sim, você vai ter que

se preocupar que... se esse disco vai lotando, se vai ter que ir expirando, não é, apagando coisas antigas. E não tem uma resposta mágica, pessoal, de quanto tempo, porque vai depender, obviamente, do volume de dados que você tem na sua rede e desses recursos que você tem aí de disco e o *sampling*, obviamente, que você escolheu usar, tá?

Então, começar com exemplos básicos, tá? Como a Cris falou, isso aqui são exemplos reais, tá, com nfdump, tá? Então, nesse primeiro caso aqui: "Ah, eu queria só ver quem está fazendo consultas aqui para os servidores DNS do Google", tá? Então, eu passo como parâmetro ali onde estão os meus *flows* guardados, tá? Esse é o jeitão que o nfcapd guarda, tá? Então, por ano, mês, dia, etc., lá dentro vai ter um monte de arquivinhos. E aí, eu coloco uma expressão muito parecida como a gente usaria em um tcpdump da vida, não é, uma expressão ali pcap(F). Então, eu quero protocolo UDP que tenha como destino porta 53 e destinos, esses dois IPs aí, tá? Nesse caso, só os v4s do Google, tá, o 8.8.4.4 e 8.8.8.8. E ele, basicamente, vai olhar, então, nesse período que eu especifiquei todo mundo que falou nessa porta, nesse protocolo, com esses servidores do Google, tá? Ele vai te falar total de *flows*, quantos bytes ele viu, pacotes, etc., tá? Então, simplesmente uma consulta bem simples, e ele te fala, então, quem falou, nessa coluna dos IPs aí da esquerda, obviamente, a gente [ininteligível] aí para não mostrar a rede, de onde foi tirado isso daí, quem fez essa consulta, quem falou com esses servidores DNS, tá?

Ok. Mas, e aí? Bom, mas e se a gente quisesse ver quem falou com os servidores DNS maliciosos, tá? Eu não me interesso com o Google, não é? Eu quero saber o resto, tá? Ok. Então, nós vamos fazer uma expressão um pouquinho diferente. Protocolo UDP; porta destino 53; rede de origem: a sua rede, do seu provedor, da sua empresa, da sua rede que você está interessado, não é, *src*(F) *net* tal, tal, tal; e que não tenha como destino esses IPs do Google ou um IP seu. Imagina que o seu seja o seu recursivo legítimo da sua rede. Então, basicamente, isso vai mostrar o quê? Todo mundo que está fazendo consultas DNS que não sejam para esses que você considera legítimo, desses servidores DNS legítimos. Vai... se sobrar alguém nessa história, vai aparecer mostrando: Olha, o IP tal de origem está falando na porta 53 UDP deste IP de destino X, tá?

SRA. CRISTINE HOEPERS: É. Eu acho, Klaus... Deixa eu só comentar. Eu acho que o importante aqui é pensar, não é, o que a gente estaria vendo nessa hora. Hum, provavelmente um roteador de banda larga ou uma base Wi-Fi, alguém comprometido, não é? Então, eu acho que esse é o ponto, sim. A gente está procurando uma coisa que... E qual é essa a nossa consulta? Ela é: me traga tudo menos aquilo que é ok. E eu acho que esse é um pensamento que vocês têm

que ter muito quando fazer consulta em *flows*, é: eu sei o que é o legítimo, então me mostra o que não seria legítimo, não é?

E, Klaus, o que eu queria só colocar... Teve umas dúvidas ali do pessoal, de onde esse comando estaria sendo rodado, se é linha de comando ou se é um software, tá? Então, eu acho que assim, esses exemplos aqui, o coletor era uma máquina Linux que rodava nfcapd e gravava tudo nesse diretório var/*log*/*flows*, e nfdump... é parte desse conjunto de ferramentas do nfdump, que é uma linha de comando. Você põe nfdump, onde que está esse arquivo, que é o diretório, e aí uma linha de consulta mesmo, que é especificamente, como o Klaus falou, é mais ou menos como era a linguagem, não é, como você faria uma consulta tcpdump. Então, isso aqui é altamente fácil de você fazer *scripts*, de você botar no Kron(F), de você fazer, inclusive... A maioria dessas coisas aqui a gente roda de maneira automatizada, não é, Klaus? Então, você queria comentar um pouco mais sobre como é que isso está sendo rodado, não é?

SR. KLAUS STEDING-JESSEN: É, é isso que eu queria exatamente falar. Sim, você pode 'logar' no seu servidor de coleta e fazer essas coisas na mão, certamente, mas a gente conhece vários times, pessoal, de resposta incidente que automatizaram essas consultas, botam isso em um Kron(F) da vida, tá, rodam isso de maneira periódica nessa filosofia que a Cris falou: tirando aquilo que eu sei que é ok, sobra o quê? Não é? Por exemplo, nesse caso aí de DNS. E eu quero que isso rode, sei lá, a cada X horas via Kron(F) neste servidor de coleta e me mande um e-mail. Pode ser um negócio simples assim, tá? Ops, no último e-mail veio uma consulta estranha aqui de um 'IPzinho' da minha rede de repente se comunicando com um IP... ou fazendo consultas para um servidor DNS que eu não reconheço, tá? Hora de parar, talvez ver: É necessariamente malicioso? Ah, não é malicioso. Bom, então, talvez coloque esse cara na lista dos não maliciosos, da próxima vez ele não aparece mais, não é? Ou, ops, é malicioso, preciso descobrir por que, então, esse cliente está fazendo essa consulta. E aí você se antecipa, não é, você não deixa um cliente seu entrar, não é, fazer uma fraude financeira e começar toda uma série de problemas quando você já pegou no início, não é, você já viu essa consulta DNS essa consulta maliciosa por um servidor malicioso. Então, sem dúvida, dá para automatizar bastante dessas coisas aí de linha de comando.

Bom, e o que mais, pessoal? Ah, a gente mencionou essa questão de IPs que estão falando com comando e controle de IoTs, não é, todos aqueles mirais da vida, não é, câmera de segurança invadida e por aí vai. Como é que eu conseguiria pegar trivialmente isso daí via um *Enter*, pessoal, na linha de comando? Nessa URL abaixo ali, do pessoal do urlhaus.abuse.ch, você pega... Desculpa, ali são outras fontes, não é? No exemplo que a gente usou, a gente usou aquela fonte ali,

iotcc.txt, um arquivo texto, tá? Você também automatiza isso, baixa com um Kron(F) da vida. E aí, a gente fez que tipo de consulta? Eu quero protocolo TCP nesse caso, tá, cujo destino seja um IP que esteja nessa lista. Você também... O nfdump te permite, por exemplo, nessa anotação @*include*, permite passar um arquivo. Então, esse arquivo pede ter milhares, milhares e milhares de IPs, tá? E, nesse caso, proveniente de onde? De comando e controle conformados de IoT, tá? Um *Enter*. Teve alguém na minha rede que falou com esses comandos e controles? Tá? Então, assim, é um negócio, assim, fácil, você se antecipa, tá, e merece depois, obviamente, investigação, não é, se você tiver alguma saída nesse comando, tá? Então, acho que... Então, está aí um exemplo, e tem... E só ilustrando, pessoal, que tem N fontes on-line de dados desse tipo, de alto valor, gratuitos, tá? Comandos e controles de IoT, outras coisas que você pode, de maneira automatizada, processar, não é, baixar esse dado, transformar em uma lista aí de IPs e fazer uma consulta nos seus *flows*, tá? Assim, uma maneira, assim, só usando software livre, como a gente mostrou aqui, não é?

SRA. CRISTINE HOEPERS: Klaus, até vi o pessoal comentando assim, ah, que tem ferramentas que analisam o normal e dão alertas quando tem algo que está fora do normal. O problema é definir o normal, não é? Se você pega uma ferramenta que o fabricante vai lá e diz o que é normal para ele, tá, o segredo está em você ter alguém que vai definir o que é normal para você, não é? E muitos desses comandos que a gente está dando, eles têm a ver com investigação de incidentes também, não é, que eu acho que aí é que é a importância, não é? Eu acho que um ponto grande aqui... Esse é o exemplo próximo que o Klaus vai falar, e depois a gente vai mostrar a saída desse comando aqui. Eu acho que talvez fique um pouco mais claro que aqui a gente não tem nenhuma regra, a gente não está procurando um protocolo específico, não é? A gente está fazendo pesquisas, acho que um pouco mais, assim, de volume, de tráfego, de outras coisas, não é?

SR. KLAUS STEDING-JESSEN: Esse daqui, pessoal, é o clássico, não é, que o pessoal chama dos *top talkers*, não é, os... quem são os grandes geradores de tráfego da minha rede, tá? De novo, um *Enter*, pessoal, um comando resolve isso daí, tá? Esse exemplo, de novo, a gente roda ali o nfdump, passa como parâmetro os... nesse caso, eu posso escolher um dia específico, posso escolher um mês, eu posso escolher uma hora específica, tá? E aí, eu estou pedindo para ele ordenar por bytes, eu estou dizendo assim: Limita para mim, mostre somente os *flows* que geraram 10 gigabytes de tráfego ou mais e me mostra os top 10, tá? O detalhe aqui, pessoal... Bom, sendo originado da minha rede, não é? *Src*(F) *net* rede do provedor, por exemplo, não é, e cujo destino não é a minha própria rede, o destino seria, vamos

dizer, para fora da minha rede, tá? E aí, vem o detalhe: "Ah, mas eu sei que eu tenho servidores meus aqui, Web, sei lá o quê, servidor FTP, isso e aquilo, que, sim, consomem muito tráfego regularmente". Ok, então, você pode dizer lá que... exclua esses meus servers.txt, uma lista... um arquivo que contenha os meus servidores legítimos. Tá, eu sei que esses caras consomem bastante, tá, mas tirando esses caras, quem são os *top talkers*? Tá? E aí, ele vai te produzir um relatório, não é? De novo, neste exemplo, mostrando apenas quem gerou 10 gigabytes ou mais de tráfego, tá? Ah, mas o que vai aparecer nesse relatório? Bom, talvez, você vai descobrir algum outro servidor seu que é legítimo e que você não tinha... não é, que você esqueceu de incluir lá no servers.txt, não é, mas pode ser que você esteja... você descobre um IP seu que está gerando *src*(F) contra um terceiro, tá, assim, tomando... ou o contrário, não é? Dependendo da regra que você colocar, alguém está recebendo um volume muito grande de tráfego, não é? Então, assim, de novo, é uma maneira simples de você até aprender mais sobre a sua rede, tipo, quem são realmente os meus geradores legítimos de tráfego, e quem não está nesse perfil merece uma investigação, tipo, esse tráfego, ele existe, não é, por que eu estou vendo tanto tráfego assim sendo originado de um IP da minha rede, tá? [Você quer avançar aí?]

Olha, um exemplo real, tá, pessoal, em uma rede aí de produção. Usando essa linha, o que se descobriu? Primeiro ofensor ali da rede, ele tinha... ele sozinho produzia 1,4 terabytes, tá? Produziu 983 milhões de pacotes, tá? Então, você vê, algo simples, como a gente comentou, isso pode ser gerado via um Kron(F), é um relatório diário que você pode receber e merece atenção descobrir: Vem cá, por que esse IP aí gerou tanto tráfego assim, não é? Então, ele sozinho gerou 206 megabits por segundo de tráfego contra terceiros aí. [Você quer avançar aí, Cris?]

Então, referências, pessoal. Como eu comentei, a RFC, tá, que fala de IPFIX; *netflow*, não é, e, no caso, de Cisco; o nfdump, que a gente gosta bastante; NfSen, que seria essa ferramenta, vamos dizer, gráfica, não é? O pessoal perguntou um pouco de... "Ah, mas como é que eu posso ver de maneira gráfica?". O NfSen não está sendo muito mais mantido, tá, pessoal, mas quem quiser, dá uma olhada. Opções aí... links específicos de Mikrotik e Juniper, tá? Recomendo fortemente, tá, vocês olharem essa apresentação do pessoal de... do time de Respostas de Incidentes da Unicamp, tá? Foi uma apresentação muito bacana no GTR e GTS... no GTS-26, na verdade, mostrando como é que eles estão usando isso no dia a dia deles, tá, pessoal? Então, assim, não é um negócio: "Ah, é impossível de usar isso daí", ou muita gente questiona se é útil. Assim, olhem essa apresentação. Vocês vão ver que, assim, muitos incidentes só foram descobertos e solucionados

graças a uma ferramenta de *netflow* na rede, tá? Então, acho que é simples assim.

SRA. CRISTINE HOEPERS: Klaus, eu acho que a gente está... são 11h35, não é? Valeria a pena... Tem várias perguntas que, talvez, fica mais claro aqui, não é? O pessoal perguntou: "Ah, tem como saber número de pacotes?". Pessoal, essa saída aqui, queria ficar um pouco mais de tempo aqui em cima, não é, se vocês forem olhar, aqui foi uma consulta, não é, como estava no slide anterior, quer dizer, ela é uma consulta que ordena por bytes, não é, agrega IPs e bytes, tem um limite que isso mostra o que gerou 10 gigabytes de tráfego ou mais, mostra os top 10 IPs, tal, mas aqui... Fui para o lado errado. Aqui, vocês já veem que ele te diz o número de *flows*, quer dizer, o número de [ininteligível], de conexões que rolaram, quantos pacotes, quantos bytes, pacotes por segundo, não é, bytes por segundo, bits por... Então, aqui, isso é muito importante, porque as perguntas todas que o pessoal... "Mas dá para ver isso? Dá para consultar?". Sim. Vocês aprendendo a--

SR. KLAUS STEDING-JESSEN: Cris, deixa eu só complementar aquele último campo, não é, porque sim, tem *bits per second*, mas aquele último campo é muito interessante, não é, que é *bytes per package*, tá? Então, por exemplo, esse é um indicativo, pessoal, que, assim, que esses pacotes... tinha bastante dado neles, tá, 1.436. Isso, muitas vezes, é um indicativo do quê? De amplificação, não é? O atacante quer gerar um tráfego amplificado, uma resposta grande, tá, e isso aqui cheira à amplificação. Então, não só o dado, eu tenho muito pacote, tá, 983 milhões de pacotes, tá, como a característica deles são pacotes grandes, que é justamente para... parece ser um ataque de negação de serviço contra terceiros. Então, você vê, uma coluna, esse detalhe nessa informação, pode já orientar como é que você vai responder ao ataque, tá, antes mesmo de ir lá atrás e ver exatamente o que está acontecendo, não é? Então--

SRA. CRISTINE HOEPERS: E, Klaus, o pessoal está perguntando: "Ah, como é que usa na realidade?". Isso aqui foi usado na realidade, tá? Isso aqui era uma rede que, várias vezes ao dia, eles têm *scripts* lá no coletor que rodam esses comandos, muito parecidos com esse aqui, e esse aqui, inclusive, e mandam por e-mail... Aquela história do *keep it simple*, não é, pessoal, do KIS, do fazer a coisa simples. O simples... "Ah, mas eu tenho que ter uma ferramenta e uma interface, e o negócio...". Não, olha só, é um *script* que está rodando em um Linux, que está coletando *flows,* que, várias vezes por dia, roda esse comando e manda as top 10 máquinas que mais estão gerando tráfego de saída, não é? Claro, excluindo os servidores. E esse foi um caso real em que eu não consigo... se eu não me engano, era um amplificador de LDAP que estava na rede, que estava fazendo parte de uma negação de serviço.

SR. KLAUS STEDING-JESSEN: Acho que era LDAP, sim, Cris.

SRA. CRISTINE HOEPERS: É, eu também acho. Se a minha memória não me trai...

SR. KLAUS STEDING-JESSEN: Cris, deixa eu só reforçar, assim, como é que usa na realidade. Olhem a apresentação da Unicamp, tá? É assim que usa na realidade, tá? E, de novo, eu acho que ter essa mentalidade KIS, *keep it simple*, não é? "Ah, mas eu preciso ter uma ferramenta mirabolante", tal. Cara, assim, um *shell script* resolve, não é? Assim, tendo as pessoas certas olhando e tomando ação, tá? Às vezes, a gente fica meio congelado nessa linha do: "Ah, mas, putz, se eu tivesse aquela megaferramenta", tal, e às vezes isso não é necessário, tá,? Basta querer fazer e usar as ferramentas que estão disponíveis, tá? Começa devagar, começa pequeno, com algumas *queries* mais simples, até para entender melhor o ambiente da sua rede, e aí vai sofisticando aos poucos, tá? Você não precisa começar logo com 150 mil alertas. Começa com um alerta: quem é o cara que hoje gerou um tráfego muito estranho, é um *top talker* que não é nenhum servidor meu que gera bastante tráfego? Começa por aí. Depois, você começa com... Por exemplo, outro exemplo interessante: Quem são máquinas da minha rede que, de repente, começaram a falar com *wallets* de criptomoeda? Opa, isso aí é sinal de mineração não autorizada de criptomoeda, não é? Em outras palavras, máquina minha comprometida por terceiros e que agora está sendo usada para minerar *bitcoin*. Você pega isso aí trivialmente via uma consulta no seu *netflow*, não é? Então, assim, de novo, aquilo que a gente está falando, é questão de telemetria e saber o que está acontecendo na sua rede, tá?

SRA. CRISTINE HOEPERS: Klaus.

SR. KLAUS STEDING-JESSEN: E, de novo, começa devagar, não é, e vai expandindo na complexidade desses testes aí. Pode falar.

SRA. CRISTINE HOEPERS: Na linha do KIS, dá para ver, assim, acho que o pessoal que não mexe muito com *shell script*, tal, fala: Ah, mas como eu faço para mandar por e-mail? Como é que eu faço para fazer tal coisa? Aí tem o pessoal: Dá para fazer consulta por pacote, por byte, por isso? Sim, o nfdump, ele é muito poderoso. Praticamente tudo que você pode fazer no tcpdump você pode fazer ali. Você pode consultar por pacotes, por bytes, agregar... dá para fazer um monte de coisa, mas, no fundo, rodar e mandar por e-mail é um *shell script* ou um *pipe*, não é, *mail* e manda.

SR. KLAUS STEDING-JESSEN: Um *pipemail*(F) você faz o quão complexo você quiser, não é? Tinha uma dúvida do que era o BPP, é bytes *per package*, tá? Então, assim, dado os pacotes que eu vi, a média dos pacotes que eu vi, eles tinham que tamanho, não é? Qual é o *payload* deles em tamanho? Tá? Isso é interessante. Quer dizer, é

como a gente falou, nesses ataques de amplificação, nesse caso eu acho que era um LDAP que estava sendo explorado, as respostas eram grandes justamente para gerar mais... um tráfego maior, não é?

SRA. CRISTINE HOEPERS: E que eu acho que é isso o que a gente comenta, assim, de você usar, porque imagine que você tenha na sua rede... Se você está olhando esse tipo de tráfego, você consegue identificar na hora, não é? Imagina que você tem uma máquina gerando 1,4 terabytes de saída da sua rede. Não tem como isso não estar afetando de alguma maneira, a menos que você seja uma rede que, sei lá, o seu *backbone* é muito grande. Então, assim, o que eu acho é que é importante pensar nessas soluções simples, não é? Então, acho que até, Klaus, recapitulando um pouco, não é, a gente aqui, falando em usar *netflow,* das várias perguntas, dos exemplos que a gente deu aqui, o primeiro: procurar acesso a alguma coisa que você não sabe muito bem o que é. Tipo, eu não sei qual é o servidor DNS malicioso de hoje, porque os atacantes estão mudando isso. Então, eu faço uma consulta dizendo: Tá, quem fez consulta para esse protocolo, tirando os meus servidores e o Google, e o Quad9, e o 1.1.1.1, quer dizer, os que seriam os legítimos, não é? E, às vezes, você vai refinando essa regra por um tempo. E aí, é interessante, voltando ao que o Klaus falou, a apresentação da Unicamp, lá eles discutem inclusive isso, quanto tempo levou para refinar as regras de *netflow*, não é, como é que foi colocar isso no ar. Nesse caso aqui, é o que o pessoal falou do IoC, eu tenho um indicador de comprometimento, que são as *botnets* de IoT ou são esses outros IPs maliciosos, incluindo *botnets* e tal. E aí, você dizendo: "Tá, eu quero saber todo mundo que entrou em contato com isso aqui, não me interessa quem da minha rede é, eu quero saber quem entrou em contato", e nesse caso aqui, você não sabe nem o protocolo, nem o IP, mas é muito estranho você ter uma máquina da sua rede que não é um servidor gerando tráfego, por exemplo, muito volumoso, não é? E aí, você gera esse alerta.

SR. KLAUS STEDING-JESSEN: Eu acho que você falou uma coisa importante, Cris, que é refinar, tá? Essa primeira linha me chamou atenção? Chamou. Tem todos os dados que eu preciso? Não. Como é um negócio agregado, eu não estou vendo portas, por exemplo. Que portas estamos falando? Bom, aí, eu volto lá no meu coletor e começo a refinar as buscas, não é? Ah, tá, então me mostra todo o *flow* que só aparece esse IP, o da esquerda ali. Ah, tá, agora, eu vou conseguir entender para quem ele estava respondendo, que portas estão envolvidas. E assim você vai refinando, não é? O problema que a gente vê hoje em muitas redes é que elas estão absolutamente cegas. "Ah, tem algo acontecendo". Como é que você sabe? "Ah, o usuário ligou, disse que está lento". Tá, mas e aí? O que mostra a sua monitoração, a sua telemetria? "Ah, não sei, não tenho, não... parece que está tudo ok". Mas parece que está tudo ok em base no quê? "Ah,

em um MRTG que eu olho aqui e parece que a banda está ok". Mas o que mais você tem? E aí, silêncio, não é? Então, essa é a hora de você ter uma rede instrumentada que consiga responder essas coisas, não é? Tá, deixa eu me debruçar sobre o problema e ver se eu consigo mais detalhes, não é? E é nessas horas que você precisa já ter isso azeitado, já ter isso funcionando, e não no desespero, "putz, meu Deus, parou de funcionar, estou sendo atacado", coisa e tal, "agora eu vou implementar esse negócio", não é? Então, acho que essa é uma mensagem importante aí que a gente queria deixar.

SRA. CRISTINE HOEPERS: É. E até para quem gosta de *buzzwords* assim, não é, hoje você pode usar *netflow* para fazer *threat hunting*, não é, que é o *buzzword* do momento. Já não é mais [ininteligível], tal, é você... Isso daqui são... todos esses comandos que a gente colocou são exemplos de fazer *threat hunting*, de você caçar ameaças na sua rede. Quer dizer, você, proativamente, vai lá e tenta procurar o que tem de problema, o que pode estar tendo de tráfego estranho e você caçar essas coisas. Quer dizer, sai uma vulnerabilidade dizendo: Olha, tinha *malware* tal que acessa porta tal, ou que acessou esse comando e controle. Vai lá no *netflow* e vê se alguém da sua rede acessou. Quer dizer, é usar ele como essa imagem, não é?

E a gente teve várias perguntas da parte... ah, legal, marco civil, tal. Uma das coisas que é bom pesar, assim, é que a parte de legislação, ela não é tão exata que nem a nossa parte de exatas aqui, não é, porque, se for pensar, tem uma lei de 1996, que é a Lei de Escuta Telemática, não é, e que ela diz que você não pode ter ferramentas de escuta telemática, o que significa que se você fosse simplesmente pegar a lei sem o contexto do uso da ferramenta, ninguém poderia ter *firewall*, ninguém poderia ter IDS na rede, ninguém poderia ter nada, não é? É bom lembrar que, para a segurança e desde que você não esteja guardando de uma maneira que facilmente você vai registrar o que um usuário está fazendo, você está guardando esses *netflows* por um tempo restrito para conseguir fazer a parte de segurança, não é, Então, assim, você não está fazendo, lá no cadastro com o nome do seu usuário, botando todos os *flows* do que ele fez, não é? Essa é uma ferramenta que se você tem isso bem documentado do porquê você colocou no ar, por que você instalou, que não é especificamente em cima de um serviço, o prazo que isso é mantido, até pelo volume de *Logs* que isso vai gerar, vocês não vão poder manter isso por meses ou anos, não é? Então, assim, *netflow*, ele é um pouco mais reduzido, essa janela, mas é muito importante para segurança, para detectar vazamento de dados, para detectar problemas de segurança aí.

Klaus, eu acho que era isso que eu queria comentar das perguntas que eu vi aí, um pouquinho...

SR. KLAUS STEDING-JESSEN: Maravilha, maravilha.

SRA. CRISTINE HOEPERS: Alguém perguntou aqui se esse PDF da Unicamp alguém conseguiu abrir. Eu abri ele ontem, tá, pessoal? Ele foi de um GTS e estava no ar ontem à noite. Então, assim, só para dizer que eu chequei todas as URLs aí, tá? Klaus, com você.

SR. KLAUS STEDING-JESSEN: Vamos avançando, então. E aí, pessoal? Então, para a gente, além do básico, não é, quer dizer, o que a gente poderia, então... A gente martelou muito nessa questão de múltiplos fatores de autenticação, não é, eu acho que isso aí é a mensagem principal aqui, mas e o que mais, tá? Então, assim, a nossa sugestão aqui... Onde é que a gente pode adotar protocolos mais modernos, não é, pessoal? Eu acho que começa assim: mandatório, tá, em tudo que você tiver de servidor Web na sua organização, tá? Hoje, de novo, o ano é 2021, não tem mais uso de http apenas. Bom, todo mundo está vendo aqui, não é, que você abre um *browser* hoje em dia e tenta acessar uma URL http, o *browser* já reclama, não é? "Opa, isso aqui não é seguro", tá? Então, essa seria uma primeira sugestão, https mandatório. Por mandatório é o quê, pessoal? Acessou porta 80, toma um *redirect* automático para 443, tá? Então, assim, não ter aquela história do: "Ah, ele é http, mas também pode ser acessado via https", tá? Então, por mandatório é isso, ele força o uso de https, tá? O que seria um objetivo? É ter *Foward Secrecy*, depois a gente vai ver isso em um testador do SSL Labs, tá? Isso protege o seu... o cliente seu que está acessando, tá, impede quebra de cripto mesmo que o tráfego tenha sido capturado, tá? Então, isso é uma boa prática. De cara, eu já encorajo a todo mundo a tentar mover coisas legadas e coisas que são http *only* para https, tá?

Outra coisa é que, assim, de cara, assim, já seria interessante usar hoje em dia, pessoal, DNSSEC, assinar todas as zonas de vocês, tá? A gente tem sorte aqui, no Registro.br, todos... Bom, primeiro que o .br foi uma das primeiras ccTLDs a ter DNSSEC há muitos anos atrás, tá? Hoje em dia, qualquer domínio que você tiver abaixo do .br, não é, qualquer coisa, você pode ter... habilitar DNSSEC. Algumas são até obrigatórias, tá, mas eu digo: Você tem o seu .com.br da vida, você vai lá e assina a sua zona, tá? O que isso te ajuda, tá? Proteção contra *cache poisoning*, e aí, sim, *cache poisoning,* para quem estiver verificando, para quem estiver validando essa sua zona, e outra coisa: DNSSEC, pessoal, ele funciona como um validador, um habilitador de outras tecnologias, tá? "Ah, eu queria ter DANE". Bom, para isso você precisa de DNSSEC, tá? Então, tem certas coisas que são pré-requisito, tá, e aí o cara morre na praia, porque, "putz, precisava ter DNSSEC", tá? Então, assinem zonas com DNSSEC. "Ah, mas eu tenho um monte de domínios". Começa com alguns. "Ah, mas eu não tenho segurança se eu vou fazer a coisa correta ou não". Começa com alguma zona

menos crítica, começa com o negócio de teste. Depois você vai indo, tá? Então, essa é outra sugestão que a gente teria.

Parte de segurança de e-mail, pessoal, tá? STARTTLS. Isso aí, hoje em dia, é trivial fazer em *post fix*, em qualquer coisa, tá? Usem coisas como DANE, tá, DMARC, DKIM, SPF, tá? Então, nessa parte de segurança de e-mail eu acho que isso é quase que mandatório hoje em dia, tá? Então, eu acho que é outra coisa importante.

Na parte de IP, pessoal, eu encararia assim, ó, pessoal: v6, hoje em dia, é protocolo corrente. Encarem v4 como legado, tá? "Ah, mas o v4 ainda vai durar sei lá quantos anos". Sim, sim, mas encare ele como legado, tá? Ele já acabou, tá, novas redes têm que pensar, sim, em v6. Outra coisa, v6 não é só habilitar *dual stack* no servidor, é pensar que ferramentas que você usa para gerência da sua rede têm suporte para v6? É aquele banco de dados que tinha lá um campo IP. Esse campo IP aceita v6? Tá? A gente ouve muito essa história: "Ah, mas eu tenho v6 na minha rede há dez anos". Sim, mas metade das suas ferramentas não suportam v6. Tem grandes redes, por exemplo, que morrem na praia com a parte de provisionamento, não é? "É, eu até teria v6, mas o cliente não consegue subir no clique-clique uma VM nova, porque o negócio não está devidamente integrado com a parte de v6". Então, pensar nisso também, tá, encarar v6 como protocolo. Muita gente fala: "Ah, pois é, o futuro...". Não, não, mudem o *mindset* disso aí, pessoal, IPv6 é agora, é o atual, tá? O v4 é um protocolo legado, tá, que sim, a gente ainda vai conviver com ele, mas a ideia do pensar é que assim, ele está... fez em alta assim, tá? Eu acho que essa seria a maneira de encarar isso aí, tá?

E na parte de segurança de roteamento, RPKI, tá? Então, tem... O pessoal do Ceptro tem feito N treinamentos, tem feito um esforço grande para levantar a barra e fazer com que as pessoas habilitem, tá... que os provedores habilitem e comecem a usar RPKI, tá?

Então, acho que isso seria... Se fosse para sumarizar, vamos dizer, o que a gente acha aí de próximos passos, é cobrir todo esse quadro aí, pessoal. Não sei se você quer comentar algum em particular aí, Cris, que você acha que é mais importante.

SRA. CRISTINE HOEPERS: Não, eu acho que, assim, a gente precisa mover para essa área, não é, a gente tem muito ataque com e-mail, muito *Phishing* ainda, muita coisa. Uma parte, assim, que hoje é interessante é que tem algumas empresas fora do Brasil da área de seguros mesmo, não é, seguros contra fraudes e *ransomware*, tal, que elas estão começando a olhar isso daí, se as organizações usam DKIM, SPF, DMARC, a gente tem países como a Holanda que o governo é obrigado a usar DANE, não é? Tinha uma pergunta no chat ali se tinha alguma apresentação sobre DANE. Eu estou tentando achar, mas eu lembro de um GTS em que o Frederico Neves, aqui do Registro, ele

apresentou, era SMTP fortificado, e-mail fortificado, onde ele mostrava como usar DANE e STARTTLS para usar com e-mail, não é? Então, tem muita coisa aí. E eu acho que IPv6, é a hora... Tinha muita pergunta sobre ataques em IPv6. Gente, é igual. A gente nota o pessoal reportando menos, porque o pessoal está vendo menos e, como diz o Klaus, às vezes, as ferramentas, não é? O pessoal está lá fazendo compra daquela megaferramenta para IDS, isso e aquilo... Tá, mas suporta IPv6, não é? Isso já passou da hora, não é, de suportar IPv6, essas coisas aí. Eu acho que era mais esse comentário aí.

SR. KLAUS STEDING-JESSEN: É como você falou, na parte de IPv6, não é que vai ele, por si só, aumentar a sua segurança. A segurança é a mesma, tá? A questão que eu vejo hoje em dia, principalmente na resposta a incidentes é assim: não passa um dia em que a gente não notifica uma rede dizendo assim: "Olha, parece ser uma máquina sua comprometida originando um tráfego estranho. Por favor, dê uma olhada". Aí a resposta qual é que é? "Hum, isso está atrás de um NAT. Não tenho *Logs*. Não sei quem originou esse tráfego malicioso", tá? Então, de cara, imagina que em um cenário em que cada equipamento seu vai ter um v6 válido, não vai ter essa do "está atrás de um NAT", o que não significa, pessoal, que você não pode implementar um conceito de filtragem, tá? Não é porque tem um v6 válido que você, administrador da rede, vai deixar esse equipamento falar ou não com qualquer um, tá? De novo, quer dizer, valem as mesmas políticas da sua organização, tá? A questão é que vai ser muito mais simples achar equipamentos problemáticos na sua rede. Eu acho que isso por si só já é uma grande vantagem, tá? [Se quiser passar aí, Cris.]

Mas, e aí, como é que eu testo alguns desses protocolos? Será que eu estou usando, será que o meu site usa, será que não usa? Tá? Então, uma sugestão: deem uma olhada no internet.nl. Bem interessante, assim, é um site do governo da Holanda em uma parceria aí com os provedores de lá. Você pode testar o seu servidor Web, tá, por vários... a parte de https, cifras, não é, a cripto que ele usa. Você pode testar e-mail, você pode testar a sua conexão, não é? Então, assim, é mais para o usuário final isso daqui, não é, para ver se o cara está usando v4, v6, etc. E comecem por aí, tá?

Outra coisa que é extremamente útil, pessoal. Fiquem com esse site do SSL Labs guardado na manga para testar... Não basta que o seu site use https, tá? Idealmente, ele teria que ter um A+ nesse teste. O que esse teste quer dizer? Se você está usando versões mais modernas de TLS, tá, TLS 1.3, TLS 1.2, se você tem alguns recursos, se vocês têm HSTS, se você está usando cifras vulneráveis, tudo isso ele avalia. Se você tem vulnerabilidades muito críticas do ponto de vista de TLS, tá? Então, assim, um objetivo seria: eu quero virar o A ou A++ nesse teste, tá, e vou... "Ah, mas como é que eu gero uma

configuração que gere A? É muito difícil". Não, você vai aqui nesse site mantido pelo pessoal do Mozilla, tá, clica ali no servidor que você tem, Apache, nginx, etc. e tal, e você pode ainda dizer: "Olha, eu quero ser *Modern*", por exemplo, aí ele é TLS 1.3 *only*. O *Intermediate* é bem razoável, tá? Ele vai gerar uma configuração com TLS 1.2 e 1.3, tá? Você pode clicar ou não ali, a história de HSTS e tudo o mais, e ele vai gerar uma configuração prontinha para você, tá? Então, assim, aquela coisa do passado que, putz, cara, você passava semanas mexendo em configurações obscuras do seu servidor Web, agora um clique aqui gera uma configuração para você. Então, isso não é mais desculpa do tipo: "Ah, não, mas, 'puta', é muito difícil virar A+ no SSL Labs", tá? E pensar que... qual que é a vantagem disso? A vantagem para os seus clientes que estão acessando... Quer dizer, você aumenta a segurança [ininteligível] os seus clientes, tá? A parte de *Forward Secrecy*, quanto que eles estão vulneráveis a alguns ataques aí se a chave do servidor for comprometida, o quanto que um atacante que estivesse vendo esse tráfego cifrado consegue abrir comunicações prévias, tá? Então, tem vantagens, tá? E hoje em dia está fácil de fazer, tá, pessoal? Eu acho que esse negócio é tranquilo, não é?

As referências estão aqui, tá, pessoal? Quando a gente fala dessas coisas aí, *tokens* de *hardware*, software, onde testar... A parte de Let's Encrypt hoje em dia não é desculpa também de "ah, mas certificado, eu não quero pagar um certificado". Trivial, você faz um cliente Acme, não é? Tem vários, Certbot, *acme-client*, e por aí vai. Então, essa parte de certificados também está bem tranquila. Muita coisa boa de tutorial de DNSSEC, o pessoal do Registro, tá? Então, assim, está fácil de você configurar, testar lá no dnsviz.net também. Toda essa parte que a Cris comentou de segurança de e-mail, tá, reputação e segurança de e-mail, DMARC, DKIM, SPF, tem um monte de tutoriais e testes para você validar a sua configuração, tá? Mesma coisa aí IPv6 e a parte RPKI, tá? Eu acho que isso seria meio que... sumarizando. Eu vou passar para a Cris, então, para outras referências, tá?

SRA. CRISTINE HOEPERS: Bom, pessoal, as outras referências eram mais lembrar para vocês, pessoal, que assim... a maioria do pessoal até citou, não é? O Gilberto está aí no chat, eu estava acompanhando, ele tem sido o evangelizador aí, tentando chegar em todo mundo, mas assim, pessoal, se vocês olharem, o que a gente comentou muito hoje é uma questão de *hardening*, não é, que é a parte de senhas, *patches.* Então, assim... Mas vamos evoluir para a segurança de roteamento, *antispoofing* e reduzir amplificação. Eu acho que isso daqui... e a gente ia dar um salto de segurança se a gente conseguir fazer isso aqui. Então, vamos continuar nesse trabalho. A gente sabe que não dá para fazer do dia para a noite, mas também a gente não pode simplesmente dizer: "Ah, é difícil, então não vou fazer".

Pessoal, a gente tem muito material, não é? O Moreiras mostrou os vídeos lá do Cidadão na Rede, mas tem outros materiais. Tudo está indexado no portal internetsegura.br, incluindo o Cidadão na Rede, a cartilha de segurança para Internet, os materiais para adolescentes, os materiais lá do jurídico, da área de uso consciente e responsável, a parte legal, material para crianças, e, pessoal, todo esse material é *Creative Commons*, não é? A gente tem, no catálogo, instruções se vocês quiserem gerar versões com a logomarca de vocês para imprimir, para fazer divulgação. E eu acho que a gente só queria mesmo era agradecer muito, não é? A gente... não sei se a gente conseguiu cobrir todas as perguntas, não é? Eu vi que teve um pessoal... eu vou até aproveitar, Klaus, e voltar aqui. Lá no início, tinha bastante gente perguntando como aprofundar em *netflow*. Pessoal, não tem lá muita coisa em português, então eu acho que português mesmo é a palestra da Unicamp, mas só isso aqui, ele já é o início, assim, do como começar. Para quem quiser uma referência interessante de segurança, esse livro aqui, tá? Ele é um livro da Cisco Press e foi escrito pelo pessoal de grupo de tratamento em incidentes da rede corporativa da Cisco, tá? Esse é um livro que ele, claro, ele tem um foco muito grande em *netflow* e nas ferramentas da Cisco de *netflow*. A Cisco, inclusive, comprou uma organização, que me foge o nome agora, que é um pessoal que teve uma das primeiras ferramentas para fazer análise, mas a parte de estudos de caso deles é focada em detecção de incidentes, em como colocar *flows* em algumas áreas da rede para capturar *flows*, e, claro, não é, para vender, você põe... que tem o *Big Data Analytics*, e põe uns nomes ali, o livro vende mais, não é, porque... mas, no fundo, é um livro de *netflow* e do uso da ferramenta lá de *netflow*.

Klaus, você quer fazer algum comentário adicional? A gente acabou já estourando o tempo, não é? Já é meio-dia. Não sei se você teria alguma coisa final para falar aí.

SR. KLAUS STEDING-JESSEN: É, não, nessa parte de aprofundar, eu acho que muitas vezes, pessoal, o pessoal, com razão, tem um pouco de receio de começar a mexer em equipamentos de produção, tá? Uma dica, talvez: comece com um *lab* pequeno, comece exportando *flow* de uma rede menor, se convença do que dá para fazer, e aí vai expandindo aos poucos, tá? Assim, você assiste a apresentação da Unicamp, vai vendo o que, daqueles exemplos, se aplica na sua própria rede e vai expandindo aos poucos. Eu acho que essa é a melhor dica nessa parte de *netflow*. Mas não deixem de usar, pessoal, tá? Eu acho que é uma ferramenta, assim, muito importante. E outra, a gente está falando de provedores, mas isso vale também para redes corporativas, tá, qualquer lugar que você possa ter, nem que seja, pessoal, para apenas ter o elemento histórico, tá? Você guarda em um canto e se um dia, se você tiver um incidente mais grave que você vai

ter que investigar, você tem dados históricos, tá? Então, pode ser, também, outra utilidade, nem que você não use nesses exemplos, vamos dizer, de consultas diárias e coisa e tal. Então, acho que basicamente era isso.

SRA. CRISTINE HOEPERS: É, até tinha... o pessoal comentou, não é, na sexta a gente vai estar lá na feira, mas não o tempo todo. A gente está meio apertado de tempo aí, então a gente não vai conseguir ficar o tempo todo. Tinha um pessoal perguntando se nfdump funciona em Debian. A gente usa em OpenBSD, em Linux, então roda em qualquer Unix(F) que vocês quiserem aí, tá?

SR. KLAUS STEDING-JESSEN: Sem dúvida, sem dúvida.

SRA. CRISTINE HOEPERS: Eu acho que eu vou passar... Da minha parte era isso. Eu queria agradecer todo mundo, não é, antes de a gente passar para o Eduardo. Obrigada a todos aí que ficaram e fizeram perguntas, e não deu para responder 100%, mas agradeço muito.

SR. KLAUS STEDING-JESSEN: Agradeço também, pessoal. A gente chegou a ter eu acho que 700 e... aproximadamente 750 pessoas aí acompanhando, tá? Foi bem bacana. Então, agradeço, mais uma vez, aí a participação de todos, e devolvo para a organização.

SR. EDUARDO BARASAL MORALES: Obrigado, Cristine. Obrigado, Klaus. Realmente, foi muito interessante, o pessoal interagiu bastante. E é aquilo que vocês falaram: se ficou alguma dúvida, algo que vocês não conseguiram responder, vão procurar ali o pessoal do CERT.br lá na feira virtual, tá? Então, ali, vai ter mais um bate-papo com alguns palestrantes. Se ficou com alguma dúvida de algum outro dia, também pode ir lá atrás do pessoal para tirar dúvida.

Bom, o vídeo de hoje, pessoal, fica no ar neste mesmo link. Então, quer relembrar, quer ver o que o Klaus falou em determinado momento? Ah, quer saber um pouquinho mais sobre, ali os *netflows*? Quer pegar aquela referência que a Cristine fez em determinado momento da apresentação? Segue nesse mesmo link, dá uma olhada, compartilhem esse vídeo. O material que eles estão utilizando ali, os slides estão disponíveis lá no site da Semana de Capacitação. Então, pode fazer download ali. As referências que eles comentaram também já são todas públicas, eles até comentaram que está tudo em *Creative Commons*, pode utilizar, replicar esse conhecimento. A ideia é que a gente divulgue ao máximo, para a Internet melhorar para todos, tá?

Agora, eu vou pedir para o pessoal lá da operação colocar o QR Code do formulário de avaliação. Lembra? São duas perguntinhas, o que a gente pode melhorar para as próximas lives aí da Semana de Capacitação, não é, qual... uma nota de zero até dez. Quer deixar

algum elogio, quer deixar ali algum comentário? Por favor, faça, tá, para a gente poder melhorar sempre aí os nossos eventos.

Bom, temos ali na sexta-feira, não é, a nossa última live da Semana de Capacitação, que vai ser sobre CDNs, então aí vai ser um punhado de gente que vai apresentar. A gente chamou as principais CDNs para explicarem como elas funcionam, como os provedores podem tirar proveito disso, como é que a Internet pode melhorar para todos. Então, a gente vai ter ali convidados como Google, Netflix, Azion, Akamai, Cloudflare, Globo, todo mundo aí conversando com vocês sobre as CDNs e como é o papel dessa infraestrutura para a Internet, não é, a importância disso, quais são os próximos passos, como as CDNs estão evoluindo. Então, participem amanhã, que é o nosso último dia. E lembrando: isso daí é na parte da manhã, não é, que a gente vai ter essa última live. Na parte da tarde, a gente vai ter a feira virtual. A partir das 14h ali às 16h, o pessoal vai estar lá interagindo com vocês. É para fazer *networking*, a gente vai ter sorteios, vocês podem conversar com os patrocinadores, então a gente vai fazer os agradecimentos. Vocês vão poder encontrar os patrocinadores, vão poder ali conversar com eles, fazer negócios, tá, e vamos ter o caça ao tesouro, não é? Já comentei aí dos brindes que vão ter ali no caça ao tesouro. Então, entrem na plataforma o quanto antes para vocês poderem participar do caça ao tesouro. Mas olha, tentou entrar agora na plataforma, não vai conseguir entrar, tem senha. A gente só vai tirar a senha no período da feira, que é a partir das 14h. Então, não adianta querer entrar antes afobado, tá? A gente vai abrir às 14h, e aí todo mundo vai poder participar, tudo bem, e interagir.

Agora, eu queria chamar o videozinho do Cidadão na Rede, não é? Como a gente comentou, se a gente consegue melhorar a segurança o mais próximo ali do usuário, o mais próximo de onde tem o problema, a gente evita os ataques, não é, como o pessoal comentou aí na live. Então, pedir aí o videozinho do Cidadão na Rede. Pode tocar.

[exibição de vídeo]

SR. EDUARDO BARASAL MORALES: Bom, gostaria de agradecer os patrocinadores, que é a Juni Link IP e Cloud Network by Giovaneli Consultoria, WZTECH Networks, ICANN, Netfinders Brasil, Novatec Editora, Solintel, Cisco e Logicalis, 4Bios IT Academy, Globo, Netflix, Fiber X, Huawei, e o apoio de mídia da revista RTI e Infra News Telecom. Bom, pessoal, muito obrigado para todos que conseguiram acompanhar a live até agora, não é, e lembrem-se de participar amanhã, que a gente vai falar sobre CDNs. Então, obrigado e até amanhã.