infra MAGAZINE

Edição 09 :: Ano I

DevMedia

ESPECIAL: Métricas de segurança
Qual é o nível de segurança da sua organização?

Por dentro do SSH
Um protocolo seguro para acesso remoto

DHCPv6
Autoconfiguração de endereços



Criptografia: Segurança para seus dados
Conheça as soluções TrueCrypt e Cryptzone



TENHA ACESSO ILIMITADO A TODO CONTEÚDO DO SITE DEVMEDIA

SEJA UM ASSINANTE MVP!

Tenha acesso garantido a qualquer tema que você possa necessitar!

VIDEOS -AULAS

O assinante MVP acessa todas as vídeo-aulas do site DevMedia. Nenhum outro produto dá essa possibilidade. São mais de **7.000 video-aulas.**

CURSOS

Nosso site possui atualmente **+ de 250 cursos online** com a qualidade que você já conhece e confia. Com o MVP você terá acesso a todos eles.

REVISTAS

Assinante MVP acessa todas as nossas revistas na versão digital, incluindo todas as edições anteriores. Quando pintar aquela dúvida você terá mais de **3.500 artigos para consultar!**

ASSINATURA MVP MOST VALUABLE PROFESSIONAL

A assinatura MVP te dá a oportunidade de aumentar seu conhecimento em diversos assuntos, com qualidade e economia.

Invista na sua carreira se torne um profissional ainda mais completo!

POR APENAS R$59,90 POR MÊS

DevMedia

Acesse: www.devmedia.com.br/mvp

Sumário

Olá, eu sou o **DevMan**! Desta página em diante, eu estarei lhe ajudando a compreender com ainda mais facilidade o conteúdo desta edição. Será um prazer contar com sua companhia! Confira abaixo o que teremos nesta revista:



Infra, Web

06 – Autoconfiguração de endereços via DHCPv6
Trabalhando com uma das principais funcionalidades do novo IPv6
[*Eduardo Barasal Morales*]

Infra, Segurança

15 – Criptografia: Segurança para seus dados
Conheça as soluções TrueCrypt e Cryptzone
[*Roberto Henrique de Sousa*]

Infra, Segurança

23 – SSH – Protocolo seguro para acesso remoto
Utilizando SSH e um protocolo Cliente/Servidor para transmissão criptografada de dados
[*Bismarck Matos de Assis*]

Infra, Segurança

30 – Métricas de segurança
Qual é o nível de segurança da minha organização?
[*Bruno Bogaz Zarpelão*]

[Infra] Artigo que apresenta tecnologias relacionadas a questões de Infraestrutura.

[Segurança] Artigo dentro do contexto de Segurança: redes, servidores, sistemas operacionais, infraestrutura em geral.

[Web] Artigos sobre ou que envolvam tecnologias de infraestrutura para WEB.

FÓRUM
DEVMEDIA

O lugar perfeito para você ficar por dentro de tudo o que acontece nas tecnologias do mercado atual



No fórum da DevMedia você irá encontrar uma equipe disponível e altamente qualificada com consultores e colaboradores prontos para te ajudar a qualquer hora e sobre qualquer assunto. Temos as salas de Java, .NET, Delphi, Banco de Dados, Engenharia de Software, PHP, Java Script, Web Design, Automação comercial, Ruby on Rails e muito mais!

ACESSE AGORA
www.devmedia.com.br/forum

DevMedia

infra MAGAZINE

Ano I • Edição 09 • 2013

Edição

Editor

Eduardo Spínola (*eduspinola@gmail.com*)

Sub Editores

Marco Antônio Pereira Araújo (maraujo@devmedia.com.br)

Rodrigo Oliveira Spínola (rodrigo.devmedia@gmail.com)

Produção

Jornalista Responsável Kaline Dolabella - JP24185

Atendimento ao leitor

A DevMedia possui uma Central de Atendimento on-line, onde você pode tirar suas dúvidas sobre serviços, enviar críticas e sugestões e falar com um de nossos atendentes. Através da nossa central também é possível alterar dados cadastrais, consultar o status de assinaturas e conferir a data de envio de suas revistas. Acesse **www.devmedia.com.br/central**, ou se preferir entre em contato conosco através do telefone 21 3382-5038.

Publicidade

publicidade@devmedia.com.br – 21 3382-5038

Anúncios – Anunciando nas publicações e nos sites do Grupo DevMedia, você divulga sua marca ou produto para mais de 100 mil desenvolvedores de todo o Brasil, em mais de 200 cidades. Solicite nossos Media Kits, com detalhes sobre preços e formatos de anúncios.

Fale com o Editor!

É muito importante para a equipe saber o que você está achando da revista: que tipo de artigo você gostaria de ler, que artigo você mais gostou e qual artigo você menos gostou. Fique a vontade para entrar em contato com os editores e dar a sua sugestão!

Se você estiver interessado em publicar um artigo na revista ou no site Easy Java Magazine, entre em contato com o editor, informando o título e mini-resumo do tema que você gostaria de publicar:

Eduardo Spínola - Editor da Revista
eduspinola@gmail.com

DevMedia

Editorial

O IPv6 segue conquistando seu espaço a cada dia. Apesar de ainda ser observado com insegurança por muitos, esse novo protocolo se apresenta cada vez mais sólido e pronto para os desafios que estão por vir. Você apostaria no IPv6? Uma das grandes bases de sucesso do IPv4 é o DHCPv4, e seguindo este mesmo raciocínio, com o IPv6 não será diferente. Pensando nisto, como destaque de capa desta edição, elaboramos um artigo sobre o DHCPv6.

Deste modo, **Autoconfiguração de endereços via DHCPv6** explica uma das funcionalidades básicas do IPv6, a autoconfiguração de endereços via DHCPv6. Os leitores aprenderão tanto a teoria como a prática sobre o assunto e, ao fim do estudo, estarão aptos a aplicar este conhecimento no seu dia a dia.

Em **Criptografia: Segurança para seus dados**, analisaremos a importância do uso de sistemas de criptografia para proteção efetiva de informações críticas armazenadas em notebooks, tablets, pen-drives, HDs externos e até mesmo em desktops que contenham informações confidenciais ou sensíveis. Para isso, conheceremos as soluções TrueCrypt (open source) e Cryptzone.

SSH – Protocolo seguro para acesso remoto apresenta as principais características do protocolo SSH, bem como as novas instalações, configurações e customizações introduzidas em seu arquivo de configuração. Serão descritos os diferentes tipos de opções e seus parâmetros padrão. Além disso, serão expostas algumas mudanças que podem ocasionar melhor desempenho e melhor segurança.

Por fim, **Métricas de segurança** discorre sobre os principais conceitos relacionados às métricas de segurança da informação. Primeiramente, será explicada a definição de métrica de segurança, juntamente com os principais atributos que uma métrica de segurança deve ter. Depois de conhecer estes conceitos, será estudado um processo de cálculo e análise de métricas de segurança, que pode ser utilizado na avaliação e na melhoria do nível de segurança de uma organização.

Eduardo Oliveira Spínola
eduspinola@gmail.com
twitter.com/Java_Magazine



Seu **conhecimento vale muito** na DevMedia

Publique artigos e vídeos gratuitamente no site e participe do programa **PayContent.**

Sua participação pode ser premiada: quanto mais você postar, mais chances de ganhar.



Para saber mais acesse:
www.devmedia.com.br/paycontent

DevMedia

Autoconfiguração de endereços via DHCPv6

Aprenda a trabalhar com uma das principais funcionalidades do novo IPv6

Em função do excesso de informação ao qual estamos dispostos nos dias atuais, basta um piscar de olhos para se sentir desatualizado. A cada instante novas descobertas são feitas e novas tecnologias são desenvolvidas, o que nos exige uma constante sincronia com essa evolução para se manter vivo num mercado cada vez mais competitivo. Ou seja, o constante aprendizado se torna questão de existência para um profissional de qualquer área, de forma que simplesmente abster-se de acompanhar essa evolução o tornará obsoleto em pouco tempo.

Na área de redes de computadores, o assunto mais proeminente no momento é o novo protocolo de internet – o IPv6. Este protocolo foi criado com o intuito de prover suporte ao crescimento expansionista da internet, meta que o protocolo antigo, o IPv4, não permite alcançar.

O problema do IPv4 é uma característica intrínseca que ele possui: sua quantidade limitada de endereços que podem ser alocados a computadores distintos. Seus 32 bits de endereçamento permitem somente 4 bilhões de combinações diferentes, um número insuficiente se pensarmos que o mundo já possui aproximadamente 8 bilhões de pessoas. Em outras palavras, se cada um tiver um computador pessoal em sua casa, não será possível que todos se conectem a internet ao mesmo tempo por falta de endereços. Apenas uma parte dos usuários conseguirá entrar na rede, enquanto a outra parte deverá esperar para se conectar.

Já o IPv6 opera com 128 bits de endereçamento, o que permite mais de 11 undecilhões de combinações diferentes. Pode-se inclusive dizer que a quantidade de endereços disponíveis é suficiente para se criar uma internet IPv4 em cada estrela do universo. Isto é, se a constante de Avogadro (6x1023) que tanto estudamos

Resumo DevMan

De que se trata o artigo:

Este artigo visa disseminar o conhecimento sobre o novo protocolo de internet, o IPv6, sob o aspecto de uma de suas principais funcionalidades: a autoconfiguração de endereços via DHCPv6.

Para isso, o artigo iniciará abordando os conceitos relativos aos endereços IPv6, tais como formato, técnicas de abreviações, prefixo, ciclo de vida e classificação. Em seguida, será explicado o DHCPv6, desde detalhes do seu protocolo até seu serviço. Dessa forma, um servidor conseguirá gerenciar e distribuir endereços a outras máquinas.

Por fim, aplicaremos todos os conhecimentos aprendidos na leitura numa atividade prática. Portanto, será apresentado como trabalhar e configurar uma das ótimas ferramentas de DHCPv6: o Dibbler.

Em que situação o tema é útil:

As informações trazidas neste artigo são úteis para auxiliar na expansão do IPv6. Quanto mais técnicas forem disseminadas, mais a desmistificação sobre as dificuldades de se operar com esse protocolo será exaurida. Dessa maneira, profissionais da área de redes de computadores, ao lerem o artigo, estarão capacitados em configurar as máquinas de sua rede com o uso do IPv6 de maneira automática.

Autoconfiguração de endereços via DHCPv6:

Para que a internet continue crescendo e evoluindo, é inevitável que haja uma migração de protocolos de internet, do IPv4 para o IPv6. Isso ocasionará uma mudança no mercado de trabalho dos profissionais de rede. Eles precisarão cada vez mais aprimorar seus conhecimentos sobre esse novo protocolo. Desta forma, este artigo procurará explicar uma das funcionalidades básicas do IPv6, a autoconfiguração de endereços via DHCPv6. Os leitores aprenderão tanto a teoria como a prática sobre o assunto e, ao fim do estudo, estarão aptos a aplicar este conhecimento no seu dia a dia.

no colégio já parecia exorbitante, agora estamos tratando de um número de proporções astronômicas!

A substituição do IPv4 para o IPv6 é inevitável, e mera questão de tempo – pouco tempo! Portanto, aprender os novos serviços, os protocolos e as adaptações, é essencial para um administrador de rede que queira se manter atualizado e crescer no mercado. Com base nisso, este artigo abordará o tema DHCPv6, que é uma nova versão do DHCP para operar com o IPv6. Explicaremos tanto o conceito do protocolo como a sua ferramenta operante.

DHCP, sua importância e funcionamento

DHCP é uma sigla, em inglês, para Dynamic Host Configuration Protocol. Se fôssemos traduzir para o português, seria o equivalente a "protocolo de configurações dinâmicas de máquina".

Sua importância provém da complexidade do mundo moderno, no qual cada vez mais e mais máquinas operam e se comunicam entre si. A quantidade e a velocidade com que as informações trafegam entre elas hoje movem milhões de pessoas e empresas no mundo todo, e para que isso aconteça é fundamental que estas máquinas estejam configuradas corretamente, com endereços IP e parâmetros de rede. Contudo, configurar todas elas uma por uma de maneira manual seria impraticável e uma perda de tempo e recursos.

Por essa razão, técnicas de configurações automáticas de máquinas foram desenvolvidas. Uma delas é o DHCP, que por meio do protocolo e de uma ferramenta consegue distribuir endereços e parâmetros de rede às outras máquinas facilmente. Assim, uma máquina que queira ingressar na rede precisa somente do DHCP para se autoconfigurar, e desse modo começar a se comunicar.

O DHCP funciona por meio da arquitetura cliente servidor para intercambiar informações, na qual a máquina cliente atua requisitando dados importantes para sua configuração ao servidor. Este conhecedor dos dados da rede responderá à requisição e armazenará o estado de quem fez o pedido (cliente). Desta forma, ao final das trocas de mensagens, a máquina cliente poderá se conectar a rede e iniciar novas comunicações.

Para se operar com essa autoconfiguração via DHCP, pode-se utilizar duas versões: o DHCPv4 e o DHCPv6. Ambas são independentes e trabalham somente com os seus respectivos protocolos de internet, IPv4 e IPv6. Ou seja, se o administrador quiser trabalhar com IPv6, ele precisará utilizar DHCPv6, ao passo que se ele quiser trabalhar com IPv4, precisará utilizar DHCPv4. Neste artigo abordaremos somente o DHCPv6, deixando a cargo da curiosidade do leitor procurar explicações sobre DHCPv4.

IPv6, o novo protocolo de internet

Antes de falarmos sobre DHCPv6 é necessário que se tenha o mínimo de conhecimento sobre o protocolo IPv6. Afinal, o DHCPv6 opera somente por meio do protocolo IPv6 e somente distribui endereços IPv6. Logo, faz-se necessário introduzir alguns dos conceitos básicos do novo protocolo de internet.

Endereço IPv6

O endereço IPv6 é formado por 128 bits dispostos em oito campos. Os campos são separados pelo caractere ":" (dois pontos) e cada um deles é composto por quatro números hexadecimais. Por exemplo, 2001:0db8:1234:b010:d0ce:5678:c0ca:da9f.

O número hexadecimal em sua definição é representado por quatro bits que variam de valor, formando 16 combinações possíveis. A partir dessas diferentes combinações, o número hexadecimal pode receber desde o valor de 0 até 9 ou de A até F. Para as letras, uma consideração precisa ser feita com relação a sua escrita: tanto maiúsculas como minúsculas são aceitas igualmente em um endereço IPv6. Na **Tabela 1** está apresentada a conversão de quatro números binários para um hexadecimal (além disso, adicionaremos uma coluna em decimal para ajudar no entendimento).

Neste momento, o leitor deve estar refletindo sobre como estão dispostos os 128 bits dos endereços IPv6. Percebe-se que os 128 bits estão colocados de maneira oculta nos 8 campos. Primeiramente recorde que cada um dos campos contém 4 hexadecimais e que estes são compostos por 4 bits. Dessa forma pode-se realizar o seguinte cálculo: 8 campos * 4 hexadecimais * 4 bits = 128 bits.

Decimal	Binário	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Tabela 1. Conversão entre binário, decimal e hexadecimal

Como o endereço IPv6 é muito extenso, diversos erros podem acontecer ao se transcrever, como o esquecimento ou a inversão de alguns números. Com o intuito de evitar estes problemas e aumentar a compreensão, algumas regras de abreviação foram desenvolvidas.

A primeira delas é a eliminação de zeros à esquerda em cada campo. Dessa maneira, um endereço IPv6, como 2001:0db8:0012:0003:0456:789a:bc00:def0, pode ser reescrito da seguinte maneira: 2001:db8:12:3:456:789a:bc00:def0 (a cor vermelha destaca onde a regra poderá ser aplicada). Observe que os zeros à direita e no meio de cada campo, escritos em verde, se mantiveram de maneira igual após a aplicação da regra.

A segunda ocorre quando existe um campo composto somente por caracteres zeros. Neste caso, todos os quatro zeros do campo podem ser representados por um único zero. Logo, um endereço IPv6 2001:0db8:0000:ded0:0000:ba7a:ca1a:b0ca ficaria assim: 2001:0db8:0:ded0:0:ba7a:ca1a:b0ca (a cor vermelha e a azul servem para mostrar a transformação com a aplicação da regra).

A terceira e última é uma regra especial que só pode ser utilizada uma única vez na representação do endereço IPv6. Quando houver campos contíguos de zeros, estes poderão ser trocados pelos caracteres "::" (dois pontos, dois pontos). Portanto, um endereço IPv6 2001:0db8:0000:0000:0000:dad0:0000:0000, com a aplicação da regra, resultaria em: 2001:0db8::dad0:0000:0000 (a cor vermelha destaca onde a regra poderá ser aplicada e a verde, a sequência de zeros que se manteve igual após a aplicação da regra).

Caso se tentasse colocar mais de uma vez os dois pontos juntos ("::") num mesmo endereço, se geraria uma ambiguidade. Vamos exemplificar utilizando o endereço 2001:0db8:0000:0000:ba1a:0000:0000:c0c0 (a cor vermelha destaca onde a regra poderá ser aplicada). Com a utilização da regra de maneira errada, ficaria assim: 2001:0db8::ba1a::c0c0.

Este endereço errado poderia corresponder a três outros endereços certos e distintos, 2001:0db8:0000:0000:ba1a:0000:0000:c0c0, 2001:0db8:0000:0000:0000:ba1a:0000:c0c0 e 2001:0db8:0000:ba1a:0000:0000:0000:c0c0. Por essa razão, quando há duas sequências de zeros separadas, o que geralmente se faz é abreviar, por essa regra, a maior sequência.

Quanto mais regras de abreviação forem utilizadas em um endereço IPv6, mais compreensível ele ficará aos administradores de rede, mais fácil será a sua manutenção e menor será o risco de erro. Eis um exemplo com as três regras aplicadas: a forma ampliada 2001:0db8:0000:0000:cafe:d0ce:0000:0001 se transforma na forma abreviada 2001:db8::cafe:d0ce:0:1.

Prefixo

Prefixo no IPv6, assim como no IPv4, é a maneira de se designar uma rede. A partir dele um conjunto de máquinas pode ser identificado de maneira única na internet. A vantagem de se trabalhar com prefixos é a possibilidade de se encaminhar os pacotes com baixos atrasos e alta eficiência.

O prefixo no IPv6 é representado utilizando a notação CIDR (Classless Inter-Domain Routing, descrito na RFC 4632). Ou seja, a representação é feita com o auxílio do caractere "/", que servirá para separar o endereço do tamanho do seu prefixo. Um exemplo disso pode ser ilustrado por 2001:db8:face:b00c::b0a/64. Nesse exemplo, 2001:db8:face:b00c::b0a é o endereço IPv6 e o número 64 demarca o tamanho do prefixo.

Uma observação importante que precisa ser feita é que diferentemente dos dígitos expressos no endereço (que estão no formato hexadecimal), o tamanho do prefixo é expresso em numeração decimal. Ele especificará a quantidade de bits seguidos à esquerda do endereço IPv6 que designarão um prefixo (lembre-se de que cada hexadecimal é composto por 4 bits). Portanto, um endereço IPv6 2001:db8:beba:d0:1234:baba:ca:1234/64 possuirá os 64 bits mais à esquerda compondo o seu prefixo (que será a parte 2001:db8:beba:d0 do endereço).

Ciclo de vida

Todo endereço IPv6 possui um ciclo de vida que dita a sua existência. Desde a sua concepção até o seu término, o endereço passa por determinados estados. Cada um desses estados possui suas próprias características e um devido objetivo. Na **Figura 1** está apresentado o ciclo de vida completo dos endereços IPv6 com o nome dos estados.

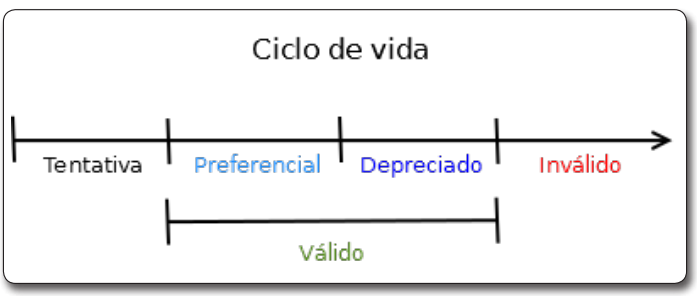


Figura 1. Ciclo de vida de um endereço IPv6

Para compreendermos o que cada estado pertencente ao ciclo de vida dos endereços faz, descreveremos em tópicos a seguir:

1. Tentativa: estado inicial no qual se verifica se já existe algum endereço cópia no enlace conectado. Neste estado o endereço ainda não foi adicionado à interface;

2. **Preferencial**: segundo estado no qual o endereço já foi adicionado à interface e pode ser utilizado tanto para iniciar uma comunicação como para receber. O tempo que um endereço pode permanecer nesse estado é configurável no DHCPv6;

3. **Depreciado**: terceiro estado no qual o endereço só pode ser utilizado nas comunicações pré-existentes (já instanciadas), porém não se pode utilizá-lo para criar novas comunicações;

4. **Inválido**: quarto estado no qual o endereço não pode ser utilizado em nenhuma comunicação;

5. **Válido**: estado que engloba o preferencial juntamente ao depreciado. O tempo que um endereço pode permanecer nesse estado também é configurável no DHCPv6.

Classificação dos endereços

Os endereços IPv6, de acordo com suas características, podem ser categorizados em três classes: Unicast, Anycast e Multicast. Cada classe possui um propósito específico numa rede IPv6, e por isso é preciso conhecê-las antes de se trabalhar com eles.

Unicast

Os endereços Unicast são utilizados para fazer a identificação única de uma interface. Deste modo, os pacotes podem trafegar com origens e destinos específicos indicando cada interface de máquina.

Dentro do escopo Unicast existe uma subclassificação que especificará ainda mais este tipo. Citaremos alguns:

• **Global**: indica que o endereço é único no âmbito global e roteável na internet. Todos os endereços pertencem à faixa 2000::/3;

• **Link Local**: indica que o endereço é único no enlace e não pode ser roteado. Todos os endereços possuem o prefixo fe80::/64.

Anycast

Os endereços anycast são utilizados para designar um grupo de interfaces, na qual só a mais próxima da origem responderá ao pacote endereçado a essa classe. Além disso, não existe um prefixo especial para os endereços anycast, basta uma configuração nas máquinas para criá-los.

Multicast

Os endereços multicast são utilizados para identificar um grupo de interfaces (uma ou mais), podendo ser de máquinas distintas. Pacotes enviados com o destino a um endereço multicast serão entregues a todas as interfaces participantes do grupo.

Para o DHCPv6, dois endereços multicast são importantes:

• ***All_DHCP_Relay_Agents_and_Servers*** (FF02::1:2): endereço utilizado pelo cliente para que suas mensagens atinjam todos os relays e servidor DHCPv6 que estiverem conectados no enlace;

• ***All_DHCP_Servers*** (FF05::1:3): endereço utilizado pelos relays para retransmitirem as mensagens dos clientes aos servidores e outros relays DHCPv6 (que não estão conectados no enlace).

Principais mudanças comparado com o IPv4?

Diferentemente do endereço IPv6, o endereço IPv4 é escrito em quatro campos com valores decimais separados pelo caractere "." (ponto). Além disso, a representação dos números dos endereços é feita em decimal, podendo ter valores de 0 a 255. Por exemplo: 192.0.2.128.

Com relação aos prefixos IPv4, estes possuem a designação de máscara de rede para separar a parte da rede pública, das subredes e das máquinas. No IPv6 esse recurso não existe.

Quanto à classificação dos endereços, o IPv4 trabalha com uma classe que não existe mais no IPv6, o broadcast. Esta mudança impacta no funcionamento do DHCP, pois a versão 4 opera com broadcast, enquanto que a versão 6 utiliza multicast.

DHCPv6, a nova versão do DHCP

O termo DHCP designa duas coisas que funcionam em conjunto, mas que são distintas: o serviço e o protocolo.

O serviço é a parte que gerencia a distribuição e a alocação de informação (endereço e parâmetro de rede). Para que ele funcione é preciso que exista uma aplicação no cliente e outra no servidor. Do lado do cliente, a aplicação trabalhará requisitando os dados e interpretando as respostas do servidor. É ele que autoconfigurará a máquina do cliente. Do lado do servidor, a aplicação trabalhará com a configuração dos dados a serem repartidos e enviados aos clientes.

Já o protocolo transporta os dados entre o cliente e o servidor. A partir de diversas regras pré-determinadas no protocolo, as duas aplicações conseguem conversar e realizar a configuração de maneira automática.

Descrição do protocolo

O DHCPv6 é o protocolo que atua na camada de transporte utilizando pacotes UDP para transmitir informações entre o cliente e o servidor. Os clientes escutam na porta 546 enquanto que os servidores e relays escutam na porta 547 (esta é uma das mudanças desta versão para a anterior, que trabalha com o IPv4).

Na sua RFC 3315, 13 mensagens são definidas, cada uma com sua respectiva função no processo de configuração automática de máquinas. Descreveremos brevemente cada uma delas:

• ***Solicit***(1): mensagem utilizada pelos clientes para localizarem os servidores DHCPv6;

• ***Advertise***(2): mensagem enviada pelos servidores DHCPv6 para indicar que seus serviços DHCPv6 estão ativos para operar. Ela é enviada em resposta à mensagem Solicit;



• ***Request***(3): mensagem enviada diretamente a um servidor DHCPv6 para requisitar parâmetros de configuração, incluindo o endereço IPv6;
• ***Confirm***(4): mensagem enviada pelo cliente para qualquer servidor DHCPv6 disponível para confirmar se o endereço adquirido ainda é válido no enlace conectado;
• ***Renew***(5): mensagem enviada pelo cliente para o servidor DHCPv6 que forneceu os dados de configuração para atualizar os outros parâmetros de configuração e estender o tempo de vida do endereço provido;
• ***Rebind***(6): mensagem enviada pelo cliente a qualquer servidor DHCPv6 para atualizar os outros parâmetros de configuração e estender o tempo de vida do endereço provido. Esta mensagem é transmitida logo após ser detectado que nenhuma resposta foi capturada para a mensagem Renew;
• ***Reply***(7): mensagem enviada pelo servidor ao cliente por diversos motivos. Resposta às mensagens Solicit, Request, Renew e Rebind contendo os outros parâmetros de configuração e o endereço assinalado. Resposta à mensagem Information-Request contendo os outros parâmetros de configuração. Resposta à mensagem Cofirm confirmando ou não se o endereço adquirido ainda é válido no enlace conectado. Resposta às mensagens Release e Decline para informar que elas foram recebidas corretamente;
• ***Release***(8): mensagem enviada pelo cliente ao servidor para informar a este que o cliente não utilizará mais um ou mais endereços assinalados;
• ***Decline***(9): mensagem enviada pelo cliente ao servidor para informar que um ou mais dos endereços assinalados já estão em uso no enlace conectado;
• ***Reconfigure***(10): mensagem enviada pelo servidor ao cliente para informar que existem novos dados de configuração. O cliente, portanto, deverá iniciar o processo Renew/Reply ou Information-Request/Reply para receber estas atualizações;
• ***Information-Request***(11): mensagem enviada pelo cliente ao servidor para requisitar informações sobre os outros parâmetros de configuração, sem o pedido de endereço IPv6;
• ***Relay-Forw***(12): mensagem enviada pelo relay ao servidor ou a outro relay para retransmitir as mensagens emitidas, ou por uma máquina cliente ou por outro relay. As mensagens retransmitidas são encapsuladas no cabeçalho desta mensagem;
• ***Relay-Repl***(13): mensagem enviada pelo servidor ao relay para ser retransmitida ao cliente. Esta mensagem contém a mensagem que deve ser entregue ao cliente encapsulada em seu cabeçalho.

Descrição do serviço

O serviço DHCPv6 pode ser executado em dois modos: o stateful e o stateless. No primeiro, o DHCPv6 trabalha com a distribuição de endereços IPv6 registrada em log. Ele manterá também o estado do cliente que está recebendo a informação. Ou seja, ele armazenará o endereço e seus atributos distribuídos, assim como os dados sobre qual máquina os recebeu.

Já no segundo, o DHCPv6 trabalha com a distribuição de outros parâmetros de rede que não serão armazenados em logs. Nenhum dado sobre o estado do cliente é mantido. Por causa disso, não há controle sobre os dados trafegados.

Este artigo focará no modo stateful, pois queremos trabalhar com a entrega de endereços IPv6. Logo, só descreveremos o procedimento e as configurações relativas a ele.

Procedimento: como o serviço funciona

O procedimento de operação do serviço de DHCPv6 é iniciado na aplicação da máquina do cliente. Esta enviará uma mensagem Solicit à rede à procura de servidores DHCPv6 (destino multicast All_DHCP_Relay_Agents_and_Servers) que possam informar os dados para autoconfiguração. Caso um relay DHCPv6 seja encontrado, este retransmitirá a mensagem Solicit encapsulada na mensagem Relay-Forw (destino multicast All_DHCP_Servers) até encontrar um servidor.

Quando um servidor recebe essas mensagens, ele responde com uma mensagem Advertise ao cliente se apresentando para operar. Caso exista um relay no caminho, a mensagem Advertise será encapsulada na mensagem Relay-Repl para ser retransmitida.

O cliente, ao receber as respostas Advertise de todos os servidores habilitados, escolherá um deles para se comunicar. A partir disso ele enviará uma mensagem Request para firmar a troca de dados para a autoconfiguração. O endereço de destino continuará sendo o multicast, contudo, um campo na mensagem, server identifier, identificará o servidor escolhido. Da mesma maneira que na primeira mensagem, se houver um relay DHCPv6 no caminho, essa será também encapsulada na Relay-Forw ao ser retransmitida.

O servidor, ao receber essa mensagem, irá então armazenar em log os dados do cliente e responderá com uma mensagem Reply informando o endereço e seus atributos para autoconfiguração. Além disso, se houver um relay DHCPv6, esta mensagem será encapsulada em uma mensagem Relay-Repl para alcançar o cliente.

Por fim, o cliente, ao receber essa última mensagem, começará a autoconfigurar sua interface de rede.

Tutorial



Atividade prática

Neste tópico aprenderemos como instalar e operar com o DHCPv6. Existem diversos aplicativos que realizam este serviço, contudo escolheu-se um que apresentava as funcionalidades do IPv6 bem implementadas.

Há implementações para diversos sistemas operacionais como Windows, Linux e MAC, cuja instalação é simples e intuitiva. Neste artigo trabalharemos com o Linux Ubuntu.

Equipamentos

Para realizar a autoconfiguração de endereços IPv6 via DHCPv6, utilizaremos três tipos de equipamentos: servidor, roteador e computador. Todos com o sistema operacional Ubuntu na versão 11.10 e o Dibbler na versão 0.8.2. Na **Figura 2** estão apresentados os desenhos esquemáticos que representam cada equipamento que será utilizado nas experiências.



Figura 2. Equipamentos para configuração DHCPv6

Instalação do Dibbler

Antes de começar a instalação é preciso verificar se a ferramenta já está instalada nas respectivas máquinas e qual é sua respectiva versão. Para isso, em cada uma das máquinas, digite os seguintes comandos num terminal:

```
$ dibbler-client help
$ dibbler-relay help
$ dibbler-server help
```

Para a experiência utilizaremos a versão 0.8.2 nos três serviços. Acredita-se que versões posteriores ou pouco antigas também funcionem corretamente. Na seção **Links** está apresentado o site em que se encontra disponível o Dibbler para download.

Primeira experiência

Para a nossa primeira configuração montaremos um simples experimento composto por um servidor e um computador. Para isso conecte-os por algum meio de comunicação, podendo ser Wi-Fi, cabo ethernet ou outro qualquer. A **Figura 3** mostra um desenho ilustrativo da topologia que deverá ser criada.

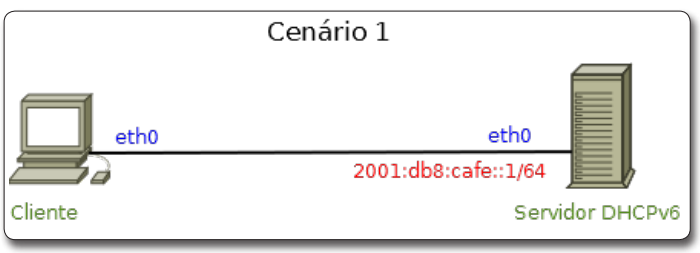


Figura 3. Cenário da primeira experiência de DHCPv6

Após criarmos a topologia de rede, é importante observar as configurações de cada uma das máquinas. Repare também as características das interfaces conectadas entre si. Assim entenderemos a troca de mensagens e saberemos quando o endereço foi adicionado na interface do computador. Para isso, em cada uma das máquinas, digite o seguinte comando:

```
$ ip addr show
```

Após a execução desse comando, descubra qual interface está conectada em cada máquina e anote para utilizar nas configurações subsequentes.

Máquina servidor

Em seguida, trabalharemos na configuração do servidor DHCPv6. Em um terminal do servidor, edite o arquivo que se encontra no caminho /etc/dibbler/server.conf (crie-o caso ele não exista). Um editor fácil de operar é o "nano", mas existem outros, como vi, vim, emacs, pico, etc. A escolha sobre qual ferramenta de edição utilizar deve ser feita de acordo com o conhecimento do administrador de rede que está configurando. No terminal do servidor, digite o seguinte comando para abrir o arquivo de configuração em modo de edição:

```
$ sudo nano /etc/dibbler/server.conf
```

Feito isso, adicione as linhas da **Listagem 1** dentro do arquivo, já aberto para edição.

Listagem 1. Arquivo de configuração do servidor DHCPv6.

```
log-level 7
log-mode short
preference 0
iface eth0 {
   preferred-lifetime 3600
   valid-lifetime 7200
   class {
      pool 2001:db8:cafe::100-2001:db8:cafe::200
   }
}
```

A seguir, explicaremos o motivo do uso de cada uma das linhas presente no arquivo de configuração da **Listagem 1**:

- log-level 7: define o nível de detalhes das mensagens de log. O valor 7 indica que as mensagens possuirão o maior nível de detalhamento quando o serviço estiver em um estado de produção;
- log-mode short: define o modo de operação do log. O modo short é o mais recomendado para a visualização a partir dos terminais que possuem um tamanho pequeno e limitado (nosso caso);
- preference 0: define o nível de preferência do serviço DHCPv6. A máquina cliente, ao receber as mensagens de todos os servidores com essa informação, preferirá se comunicar com o servidor que possuir o menor valor dessa configuração;
- iface eth0: define o nome da interface na qual será tomada as ações do serviço de servidor DHCPv6. No nosso caso, trabalharemos com a eth0, mas o leitor deverá colocar a interface previamente anotada (usando o comando ip addr show);

• preferred-lifetime 3600: define o tempo que o endereço permanecerá no estado preferido, no caso, 3600 segundos. Isso dará uma ideia ao servidor de quando o cliente enviará uma mensagem para atualizar esse tempo;
• valid-lifetime 7200: define o tempo que o endereço permanecerá no estado válido, no caso, 7200 segundos. O valor deste campo precisa ser maior que o campo preferred lifetime, pois, como já vimos, um estado engloba o outro. Além disso, ele dará uma ideia ao servidor de quando o cliente enviará uma mensagem para atualizar esse tempo;
• class: cria um pequeno escopo para colocar o pool de prefixos e suas características na configuração do servidor;
• pool 2001:db8:cafe::100-2001:db8:cafe::200: define um range de prefixos que pode ser alocado aos clientes. No nosso caso, os endereços podem variar o final de 100 até 200.

Depois de gerado o arquivo de configuração, podemos iniciar o serviço de servidor DHCPv6. Para isso, digite o seguinte comando no terminal:

```
$ sudo dibbler-server start
```

Máquina cliente

Depois de terminada a iniciação do Servidor DHCPv6, podemos configurar o computador para requisitar o endereço IPv6.

No computador, edite o arquivo que se localiza no caminho /etc/dibbler/client.conf (crie-o caso ele não exista). Utilizaremos o editor nano, mas como já dissemos, qualquer outro pode ser utilizado. Sendo assim, no terminal do cliente, digite o seguinte comando para abrir o arquivo de configuração em modo de edição:

```
$ sudo nano /etc/dibbler/client.conf
```

Em seguida, adicione as linhas da **Listagem 2** neste arquivo, já aberto para edição.

Listagem 2. Arquivo de configuração do cliente DHCPv6.

```
log-level 7
log-mode short
iface eth0 {
   ia
}
```

A seguir, explicaremos o motivo do uso de cada uma das linhas presente no arquivo de configuração da **Listagem 2**:
• log-level 7: Essa linha possui a mesma explicação que a linha respectiva definida na **Listagem 1**;
• log-mode short: Essa linha possui a mesma explicação que a linha respectiva definida na **Listagem 1**;
• iface eth0: Essa linha possui a mesma explicação que a linha respectiva definida na **Listagem 1**. Contudo é preciso trocar pela interface anotada para a máquina do cliente;
• ia: representa uma requisição de um cliente a um simples endereço IP.

Vale destacar que a linha stateless precisa estar comentada, pois ela habilita outro modo de operação que não permite requisitar o endereço IP.

Depois de gerado o arquivo de configuração, podemos iniciar o serviço de cliente DHCPv6. Para isso, digite o seguinte comando no terminal:

```
$ sudo dibbler-client start
```

Depois que o serviço tiver iniciado, acontecerá uma troca de mensagens entre o cliente e o servidor até que culmine com a distribuição e a alocação de um endereço IPv6.

Para observar o endereço IPv6 adicionado à interface do computador, digite o seguinte comando no seu terminal:

```
$ ip addr show
```

Segunda experiência

Neste cenário, tornaremos as coisas um pouco mais complexas e adicionaremos um roteador. Para isso o roteador deverá ser conectado entre o computador e o servidor. A **Figura 4** mostra um desenho ilustrativo da topologia que deverá ser criada.

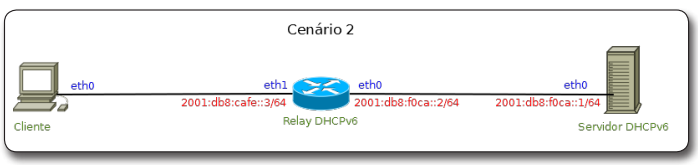


Figura 4. Cenário da segunda experiência de DHCPv6

Máquina Servidor

As configurações na máquina servidora são parecidas com a do exemplo anterior. Todavia, algumas alterações precisão ser feitas por causa da adição do relay no meio da comunicação entre o cliente e o servidor. Por causa disso, a **Listagem 3** mostrará como deve ficar o novo arquivo de configuração (este arquivo se encontra no mesmo caminho da experiência anterior).

Listagem 3. Arquivo de configuração do servidor DHCPv6.

```
log-level 7
log-mode short
preference 0
iface relay1 {
 relay eth0
 interface-id 1000
 preferred-lifetime 3600
 valid-lifetime 7200
 class {
  pool 2001:db8:cafe::100-2001:db8:cafe::200
 }
}
```

A seguir, explicaremos o motivo do uso das linhas, distintas em relação à **Listagem 1**, porém presentes no arquivo de configuração da **Listagem 3**:

• iface relay1: define o nome da interface na qual serão tomadas as ações do serviço de servidor DHCPv6. No nosso caso, trabalharemos com a relay1;

• relay eth0: especifica o nome da interface física que será utilizada para receber as mensagens do relay;

• interface-id 1000: especifica um valor que identifica a interface do servidor que recebe as mensagens do relay. Ele serve para auxiliar o servidor na detecção da interface na qual as mensagens foram geradas. Por essa razão, o mesmo valor deve ser usado na configuração do relay.

Assim como no exemplo anterior, depois de gerado o arquivo de configuração, deve-se iniciar o serviço de servidor DHCPv6. Para isso, digite o seguinte comando no terminal:

```
$ sudo dibbler-server start
```

Máquina Relay

Antes de começar a configurar o relay, é preciso se conhecer as características de suas interfaces, para assim conseguirmos configurar o seu serviço. Para isso, digite em um terminal:

```
$ ip addr show
```

Em seguida, descubra qual interface está conectada com o cliente e com o servidor e anote para utilizar nas configurações subsequentes.

As configurações no relay devem ser feitas depois das configurações do servidor e antes das do cliente. Dessa forma, ao iniciar o serviço no cliente, todas as máquinas operarão corretamente e a autoconfiguração ocorrerá rapidamente. Para isso, no roteador, edite o arquivo que se localiza no caminho /etc/dibbler/relay.conf (crie-o caso ele não exista) com o comando:

```
$ sudo nano /etc/dibbler/relay.conf
```

Feito isso, adicione as linhas da **Listagem 4** dentro do arquivo, já aberto para edição.

A seguir, explicaremos o motivo do uso de cada uma das linhas presente no arquivo de configuração da **Listagem 4**:

• log-level 7: Essa linha possui a mesma explicação que a linha respectiva definida na **Listagem 1**;

• log-mode short: Essa linha possui a mesma explicação que a linha respectiva definida na **Listagem 1**;

• iface eth1: define a interface na qual serão tomadas as ações do serviço de relay DHCPv6. Nesse caso escolhemos a eth1, que está diretamente conectada ao cliente, mas o leitor deverá colocar a interface previamente anotada (usando o comando ip addr show);

• client multicast yes: instrui o Dibbler relay a escutar nessa interface as mensagens enviadas pelo cliente ao endereço Multicast (ff02::1:2);

• client unicast 2001:db8:f0ca::2: instrui o Dibbler relay a escutar mensagens providas para certo endereço unicast. Geralmente se utiliza esse comando para interligar mais de um relay;

• Interface-id 1000: especifica um valor que identifica a interface do relay que recebe as mensagens do cliente. Ele serve para auxiliar o servidor na detecção da interface de onde as mensagens foram geradas. Por essa razão, o mesmo valor deve ser usado na configuração do relay;

• iface eth0: define a interface na qual serão tomadas as ações do serviço de relay DHCPv6. Nesse caso escolhemos a eth0, que está diretamente conectada ao servidor, mas o leitor deverá colocar a interface previamente anotada (usando o comando ip addr show);

• server multicast yes: instrui o Dibbler relay a retransmitir as mensagens do cliente para o servidor utilizando o endereço Multicast (ff05::1:3);

Listagem 4. Arquivo de configuração do relay DHCPv6.

```
log-level 7
log-mode short
iface eth1{ # interface conectada ao cliente
   client multicast yes
   client unicast 2001:db8:f0ca::2
   interface-id 1000
}
iface eth0{ # interface conectada ao servidor
   server multicast yes
}
```

Depois de gerado o arquivo de configuração, podemos iniciar o serviço de relay DHCPv6. Para isso, digite o seguinte comando no terminal:

```
$ sudo dibbler-relay start
```

Com o serviço operante, a configuração do cliente pode ser feita, já que as mensagens serão retransmitidas corretamente até o servidor.

Máquina cliente

As configurações na máquina cliente são idênticas às do exemplo anterior. Por causa disso nenhuma configuração precisa ser alterada e, portanto basta utilizá-la. Sendo assim, repita os mesmos passos e inicie a aplicação para adquirir o endereço.

Resultados das experiências

Para entender melhor a troca de mensagens e observar as informações que estão sendo transmitidas, pode ser utilizado o programa open source wireshark. Dessa maneira, o administrador de rede conseguirá observar os erros e dar manutenção facilmente.

No sistema operacional que estamos usando, o Ubuntu, a instalação do wireshark é bem simples, bastando digitar no terminal:

```
$ sudo apt-get install wireshark
```

Em seguida, utilize o programa para capturar os pacotes que estão passando pela sua interface de rede. Dessa maneira o leitor poderá observá-los e estudá-los para compreender melhor a troca de informações utilizadas no serviço DHCPv6.

Conclusão

Neste artigo, vimos como funciona um dos modos de operação do DHCPv6, a autoconfiguração de endereços, desde o seu conceito teórico até uma aplicação prática para auxiliar no aprendizado. Contudo, existe outro modo que não foi coberto, o stateless, que possui algumas diferenças. Além disso, o DHCPv6 possui uma nova funcionalidade, chamada prefix delegation, que opera com a entrega de prefixos em vez de endereços. Todavia, esse assunto é muito extenso e precisa ser tratado em outro artigo.

Esperamos que os ensinamentos trazidos nesse artigo facilitem o ingresso do leitor ao iminente e inevitável mundo do IPv6! Inclusive, vale a pena frisar que quem quiser se aprofundar no assunto, há materiais disponibilizados pelo NIC.br conforme exposto na seção **Links**.



Eduardo Barasal Morales
ed.barasal@gmail.com
É Engenheiro de computação graduado pela Escola Politécnica da Universidade de São Paulo e trabalhou com desenvolvimento de softwares para transferência eletrônica de fundos, gestão de saúde e tarifação de telefonia. Atualmente, no NIC.br, é Analista de Projetos, ministra cursos do projeto IPv6.br e também participa do desenvolvimento de seu material didático para a disseminação de conhecimento do protocolo pelo país.

Dibbler – ferramenta DHCPv6
http://klub.com.pl/dhcpv6/#DOWNLOAD

Guia de uso do Dibbler
http://klub.com.pl/dhcpv6/doc/dibbler-user.pdf

RFC 3315 – Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
http://www.ietf.org/rfc/rfc3315.txt

Apostila "Curso IPv6 básico" do NIC.br
http://ipv6.br/download/

RFC 2460 – Internet protocol, version 6 (IPv6) Specification
http://www.ietf.org/rfc/rfc2460.txt

Núcleo de Informação e Coordenação do Ponto BR
www.nic.br

DÊ UM SALTO
EM CONHECIMENTO!



Acesse o maior portal para desenvolvedores da América Latina!

20 mil posts

430 mil cadastrados

10 milhões de page-views por mês

http://www.devmedia.com.br/

DevMedia

Criptografia: Segurança para seus dados

Perca seus dispositivos, mas não seus dados. Conheça as soluções TrueCrypt (open source) e Cryptzone

Criptografia é a arte ou a ciência de transmitir mensagens em código, de modo que somente o emissor e o receptor específico possuam as condições ou o entendimento necessário para traduzir o código criado em uma informação compreensível. O termo em si surgiu da fusão das palavras gregas "kryptós" e "gráphein", que significam algo como "oculto" e "escrever".

Esta técnica é tão segura que se a informação codificada passar pelas mãos de uma pessoa que não seja o seu destinatário original, ela se manterá incompreensível a este, garantindo assim a restrição da mensagem a um grupo específico de pessoas.

A criptografia, por mais que seja um assunto muito abordado recentemente, tem na verdade sua origem registrada séculos atrás, como na técnica usada nos hieróglifos encontrados em diversos monumentos, especialmente nas pirâmides do Antigo Império do Egito. Há mais de 4.000 anos, esta escrita foi utilizada pelos egípcios para transmitir mensagens ocultas, assim como por outros povos, que utilizaram técnicas semelhantes para manter a mensagem restrita a um grupo específico em seus impérios.

A criptografia também foi amplamente utilizada pelos impérios grego e romano, chegando à era moderna como um diferencial para vencer batalhas na Segunda Guerra Mundial, com a máquina alemã chamada Enigma.

A partir de 1930 esta máquina eletromecânica passou a ser muito utilizada pelas forças militares da Alemanha nazista com o objetivo de codificar mensagens de conteúdo secreto, especialmente referentes à movimentação estratégica das tropas e planos de ataques. A decodificação da criptografia deste equipamento sempre foi um dos grandes entraves das Forças Aliadas (Inglaterra e França). Somente após o auxílio de um grupo de cientistas poloneses que fugiam dos horrores da guerra em seu país é que os Aliados obtiveram a decodificação destas máquinas. Assim, todas as mensagens das tropas alemãs interceptadas eram compreendidas de forma bem discreta, a fim de não levantar suspeitas por parte dos nazistas. A perda desta codificação foi um dos grandes trunfos que levaram os Aliados a derrotarem a supremacia de Hitler.

Resumo DevMan

De que se trata o artigo:

Nos últimos anos temos acompanhado um aumento expressivo no número de incidentes de segurança da informação causados por perda ou roubo de equipamentos que contêm informações confidenciais de grandes organizações públicas e privadas, como também incidentes com pessoas comuns que armazenam informações vitais em um disco rígido sem qualquer preocupação ou consciência dos riscos aos quais ela se expõe. Mais do que nos proteger contra furtos, devemos nos preocupar com as consequências que a perda ou um acesso não autorizado a estes equipamentos podem nos causar. O prejuízo pode ser imensurável e irrecuperável. É sobre isso que abordaremos neste artigo.

Em que situação o tema é útil:

Com a crescente adoção de dispositivos móveis pelas organizações, um novo conceito foi desenvolvido: a Consumerização. Esta prática permite que funcionários tragam seus próprios dispositivos móveis para uso dentro da empresa, utilizando os recursos da rede e, o que é mais preocupante, transportando informações sensíveis e estratégicas, sem qualquer controle por parte dos departamentos de TI da maioria das organizações, especialmente no Brasil. Como este é um caminho sem volta, é necessário prover soluções que mitiguem os riscos de vazamento de informações ocasionados pela perda ou pelo furto destes dispositivos móveis.

Criptografia: Segurança para seus dados:

Este artigo aborda a importância do uso de sistemas de criptografia para proteção efetiva de informações críticas armazenadas em notebooks, tablets, pen-drives, HDs externos e até mesmo em desktops que contenham informações confidenciais ou sensíveis.

O que mudou de lá para cá foi a forma como empregamos a lógica da codificação. Se antes uma máquina eletromecânica como o Enigma nos auxiliava a criar e decodificar estas informações, hoje os sistemas computacionais elevaram esta capacidade ao extremo, de forma a impossibilitar a decodificação de determinados códigos sem a inserção da chave que realize a descriptografia, diferentemente do que aconteceu na Segunda Guerra.

Com base neste conceito, apresentaremos aqui dois excelentes sistemas de criptografia para atender desde as necessidades de proteção do usuário doméstico até os grandes usuários corporativos.

Tudo se compra, menos os seus dados!

Nestes últimos cinco anos, tivemos notícias bastante interessantes e até mesmo preocupantes referentes a roubo de equipamentos de informática e a vazamento de informações, que chamaram relativa atenção da mídia tradicional como também dos especialistas de tecnologia e segurança da informação. Um exemplo foi o caso do furto de dois notebooks e de um disco rígido da Petrobras contendo informações estratégicas sobre as atividades da corporação, sem qualquer proteção contra acesso não autorizado aos dados.

Outro caso similar aconteceu com a NASA, que teve um de seus notebooks furtados dentro de suas dependências. Este continha algoritmos para controle da Estação Espacial Internacional sem qualquer sistema de criptografia, dando livre acesso aos códigos a qualquer usuário. E este não foi um caso isolado, pois, segundo dados da própria Agência Espacial Americana, entre os anos de 2009 a 2011 foram roubados 48 notebooks.

Para mostrar que isso não acontece somente com grandes corporações, temos o recente e famoso caso da atriz Carolina Dieckmann, que teve diversas fotos íntimas divulgadas na Internet. Até a identificação dos reais autores e da origem da invasão que se deu por e-mail, a suspeita recaia na empresa de manutenção que havia recebido o equipamento semanas antes para realizar o seu conserto.

Por outro lado, temos um exemplo oposto de como a criptografia pode proteger com total segurança as suas informações. No caso da Operação Satiagraha, deflagrada pela Polícia Federal em 2008, foram apreendidos computadores e discos rígidos pertencentes ao banqueiro Daniel Dantas. Ao tentarem acessar os dados para coleta de provas contra o banqueiro, os peritos encontraram um sofisticado sistema de criptografia que impediu completamente o acesso. Mesmo com o apoio de peritos americanos do FBI, as informações continuam invioláveis até hoje, de modo que somente o usuário, no caso, Daniel Dantas, tem o poder de liberar o acesso por meio de suas chaves de criptografia.

Dessa forma, vemos que estas notícias nos dão argumentos suficientes para trabalhar em diversos temas, como Backup, Criptografia, Segurança Física, Controle de Acesso e Políticas de Segurança. Como pode ser visto no título deste artigo, focaremos no tema Criptografia, por ser um assunto muito debatido em teoria e pouco aplicado na prática dentro das organizações e também na nossa rotina de vida pessoal.

Interpretação técnica dos fatos

Com base nestas notícias, o que podemos concluir? Que a criptografia ainda é um assunto mal compreendido e mal aplicado! Uma grande empresa estatal que trata de assuntos estratégicos e de segurança nacional não possui uma política para proteger dispositivos móveis e muito menos para transportá-los de forma segura. Outra notícia nos mostra que o maior celeiro de estudiosos científicos, responsáveis por tratar dos assuntos mais complexos do universo, não tem conhecimento suficiente para adquirir um sistema de proteção de seus próprios equipamentos.

Também temos o caso da atriz que não tomou as devidas precauções e dos advogados mal informados que sequer sabiam por onde as fotos comprometedoras haviam vazado. Fechando o ciclo de notícias, vemos a dificuldade dos peritos em coletar informações e compreender o sistema de criptografia utilizado pelo banqueiro Daniel Dantas, que mesmo não sendo um especialista em tecnologia, adotou as práticas recomendadas, provavelmente orientado por alguém com conhecimento na área de segurança de informação.

Tais matérias e as situações descritas em cada uma delas servem de embasamento para nosso estudo, nos permitindo avaliar a extrema necessidade de adotarmos sistemas de proteção contra acessos não autorizados às informações. Em todos os casos, a maior preocupação não era com o ativo físico, o equipamento em si, mas com as informações armazenadas que acabaram sendo perdidas.

Usemos como exemplo os casos da Petrobras e da NASA. Ambas as organizações possuem em mãos todos os recursos necessários para a realização de suas atividades, recursos estes que agregam tecnologias de ponta. As duas organizações possuem inúmeros procedimentos para garantir a segurança de suas operações, como também de seus colaboradores, uma vez que ambas tratam de questões de vital importância econômica e de segurança nacional. Seus colaboradores diretos e indiretos (prestadores de serviço terceirizado, fornecedores) passam por rigorosos processos de seleção e de capacitação técnica para exercerem as atividades específicas de cada negócio e, dando suporte a tudo isso, ambas possuem uma avançada infraestrutura de TI, incluindo alguns dos supercomputadores mais rápidos em operação no mundo.

Porém, em meio a tudo isso, nem a Petrobras e nem a NASA puderam evitar o extravio de informações altamente confidenciais e de suma importância para as suas atividades. E, como vimos, isso aconteceu não pelo fato de serem alvos de hackers com elevados conhecimentos técnicos para burlar firewalls e todos os sistemas de segurança online. Para obter acesso a estas informações, bastou um pouco de astúcia para colocar o notebook debaixo do braço e apertar o botão Power. No máximo, bastaria retirar o disco do notebook e conectá-lo a outro computador para ter este acesso. Simples assim!

A falha aqui não é de tecnologia, mas de processos e pessoas. A tecnologia de criptografia está disponível a custos acessíveis para organizações de qualquer tamanho, inclusive com proteção apropriada até para um simples usuário doméstico, sem contar

com opções Open Source, como mostraremos mais adiante. O que faltou aqui foram processos, incluindo políticas de segurança, termos de responsabilidade e, principalmente, capacitação e conscientização dos colaboradores, pois qualquer pessoa bem orientada de uma forma ou de outra procuraria garantir a proteção das informações sobre sua responsabilidade.

Outro fato que nos mostra a falta de orientação adequada é o que ocorreu com a atriz Carolina Dieckmann. Hoje sabemos que o vazamento das fotos se deu pelo acesso não autorizado à conta de e-mail da atriz, que por descuido acabou deixando nos Itens Enviados do serviço de e-mail as fotos comprometedoras que a levaram a esse constrangimento nacional. Até chegarem a esta conclusão, toda a suspeita do vazamento recaiu sobre a empresa que realizou a manutenção do notebook semanas antes da divulgação das fotos.

É neste ponto que gostaríamos de chamar a atenção dos leitores. Como alguém envia um notebook contendo fotos de cunho íntimo, sem falar nas outras informações confidenciais que deveriam estar armazenadas no dispositivo (como mensagens de e-mail, informações financeiras, contratuais, etc.) a uma empresa especializada em manutenção de equipamentos de informática e não se preocupa que alguma pessoa tenha este acesso, mesmo que "sem querer"? Pior, como ela transitava despreocupadamente com este dispositivo móvel contendo estas informações sem qualquer proteção além de sua senha de login?

Muito provavelmente ela não sairia na rua com um envelope lacrado dentro de sua bolsa contendo todas aquelas fotos ou muito menos despacharia este envelope via serviço de correio, pois no mínimo haveria um entendimento de que a qualquer momento sua bolsa poderia ser roubada ou que o envelope poderia ser extraviado e aberto por qualquer curioso. Ela correu este risco porque não teve orientação adequada para operar um simples notebook, e observe que não estamos falando de conhecimentos básicos de informática para ligar, desligar, fazer uso de editores de texto, planilhas ou acessar a Internet. Estamos nos referindo a algo totalmente obscuro aos usuários comuns, que é a questão da segurança da informação.

Ao contrário do que muitos pensam, segurança da informação não trata apenas de tecnologia como antivírus, firewall, backup ou criptografia. Antes de pensar em utilizar uma dessas ferramentas, a pessoa deve entender o porquê ela deve se proteger e quais são os riscos, para somente em seguida saber que proteção usar e como usar. No caso da atriz, este notebook deveria estar criptografado para evitar a possibilidade de que um funcionário da empresa de manutenção ou mesmo um ladrão que tivesse furtado o equipamento conseguisse abrir o conteúdo dos arquivos. Mas como vimos, se nem mesmo cientistas da NASA atentaram para este fato, o que esperar do usuário comum?

Depende. Se este usuário comum for um banqueiro que sabe o valor de suas informações, certamente ele procurará alguma solução para sua proteção. É o famoso caso do banqueiro Daniel Dantas, que segundo a assessoria de seu banco Opportunity decidiu fazer uso de sistemas de criptografia na troca de mensagens por e-mail, como também no armazenamento das informações confidenciais em seus notebooks e discos externos por suspeitarem de espionagem de seus concorrentes. O mais curioso é que nesse caso ambos os softwares utilizados eram gratuitos, que como vimos funcionam muito bem.

Com a deflagração da Operação Satiagraha pela Polícia Federal em 2008, foram encontrados atrás de uma parede falsa alguns HDs que poderiam conter informações comprometedoras de todas as atividades ilegais do banqueiro que estavam sendo investigadas.

Foram apreendidos seis HDs e um notebook para passarem por uma perícia no Instituto Nacional de Criminalística (INC), porém, para "surpresa" dos peritos, todos os equipamentos estavam criptografados. Na esperança de terem acesso a estas preciosas informações do banqueiro, os HDs e o notebook foram enviados para os Estados Unidos, onde passaram por uma avaliação técnica do FBI. O resultado da análise: passados dois anos desde a apreensão, não foi possível quebrar o sistema de criptografia de nenhuma unidade.

O desconhecimento deste tipo de proteção era tão latente que, segundo notícias, os peritos do IPC afirmavam que se tratava de um novo sistema de proteção no Brasil, sendo que o conceito de criptografia utilizado por estes programas já estava à disposição no mercado há muito tempo. Na época, ambos os programas utilizados estavam disponíveis na Internet gratuitamente, entre eles o antigo sistema de criptografia criado por Philip Zimmermann em 1991 chamado PGP (Pretty Good Privacy). Este tinha como objetivo criar uma forma de proteção na troca de mensagens por e-mail. Atualmente está disponível somente em versões pagas, sob o licenciamento da Symantec.

O outro sistema denominado como TrueCrypt ainda permanece gratuito (ver seção **Links**), permitindo que qualquer pessoa possa realizar a criptografia de unidades de discos fixos, como HDs de desktops e notebooks, assim como unidades removíveis, como pendrives, memory cards e discos externos conectados via USB.

Como me proteger? Por onde começar?

Por que um banqueiro, não sendo especialista em Tecnologia e Segurança da Informação, tomou todos os cuidados necessários para não ter suas informações vazadas, ao passo que cientistas com alto grau de formação nas áreas de exatas ainda não se deram conta de tal sistema de criptografia? A resposta é porque ele soube entender que a informação é um ativo tão valioso quanto ouro e que, como tal, deve ser guardada dentro de um cofre, por medida de segurança.

Entender que a informação é um ativo de valor igual ou até superior em relação a muitos metais preciosos e saber identificá-los dentre essa enorme quantidade de dados que manipulamos, são os primeiros passos para garantir a sua proteção. Com isso podemos definir quais informações serão consideradas públicas ou restritas. Isso é parte da Classificação da Informação.

O segundo passo é garantir a sua preservação, armazenando cópias das informações que foram classificadas como objeto de

valor ao usuário. O uso de soluções de backup se faz necessário, porém somente possuir um programa de backup não é o suficiente. É preciso haver uma política de backup, o que significa que você deve criar uma rotina diária, semanal ou mensal, mas que deve ser seguida à risca. Além disso, é primordial armazenar em segurança o dispositivo que contém o backup, pois de nada adianta deixar o backup ao lado do computador que contém os mesmos dados. Se alguém invadir a sala ou se o ambiente pegar fogo, perde-se tudo.

Terceiro e último passo, criptografe suas unidades de armazenamento, estejam elas em desktops, notebooks, pen-drives, discos externos ou até mesmo em tablets. Guarde com segurança as chaves e as senhas geradas e durma tranquilo.

Qual a melhor solução? Como fazer na prática?

Há inúmeras soluções disponíveis no mercado, sejam elas proprietárias, sejam no modelo Open Source. Como o nosso foco aqui é a criptografia de unidades de armazenamento, veremos duas excelentes opções: uma voltada para o mercado corporativo e outra para usuários domésticos.

Para o mercado corporativo, a solução Cryptzone é umas das mais conhecidas e utilizadas atualmente, pela sua integração com Active Directory em ambientes gerenciados por servidores Microsoft, permitindo a gestão remota de todos os dispositivos criptografados entre eles notebooks, tablets, pen-drives e discos externos. Já para o uso doméstico, a indicação é o software Open Source TrueCrypt, o mesmo que impediu o acesso aos discos apreendidos na Operação Satiagraha pelos peritos do IPC e pelo FBI.

É compreensível que para muitos usuários comuns, o processo de criptografia possa parecer complexo, pois ele exige conhecimentos intermediários em informática, porém para os leitores da Infra Magazine pressupõe-se que qualquer uma das soluções é de fácil compreensão, ainda mais tendo todo o apoio da documentação oficial do produto presente no website de cada distribuição.

Por mais que tenhamos citado o Cryptzone para usuários corporativos e o TrueCrypt para usuários domésticos, ambas as soluções podem ser implantadas em qualquer cenário. O que os difere é a gestão do produto, pois enquanto o Cryptzone permite a centralização da administração de todos dispositivos criptografados por meio de um Console, o TrueCrypt só pode ser administrado localmente em cada dispositivo. Isso é muito importante, pois imagine a dificuldade de um departamento de TI para dar suporte a 10, 20, 50 ou 100 diferentes dispositivos móveis de usuários espalhados por diversas localidades, ainda mais tendo que se responsabilizar pelas chaves de criptografia ou reset de senhas perdidas de cada equipamento.

Cryptzone

A Cryptzone é uma empresa mundialmente conhecida pelo seu portfólio de soluções de DLP (Data Leak Prevention / Prevenção de Vazamento de Dados), e todos os seus produtos podem ser adquiridos em módulos, como a solução para proteção de servidores, desktops, notebooks (Secured eDevice), discos (Secured eDisk), mídias removíveis (Secured eUSB), troca de mensagens por e-mail (Secured eMail), arquivos armazenados em servidores (Secured eFiles) e até para a plataforma Microsoft SharePoint (Secured eCollaboration).

Todas as soluções são gerenciadas por meio de um console central chamado de SEP (Simple Encryption Platform/Plataforma de Criptografia Simples), sendo totalmente integrado ao ambiente Active Directory da Microsoft. Na **Figura 1** temos a sua tela de administração.

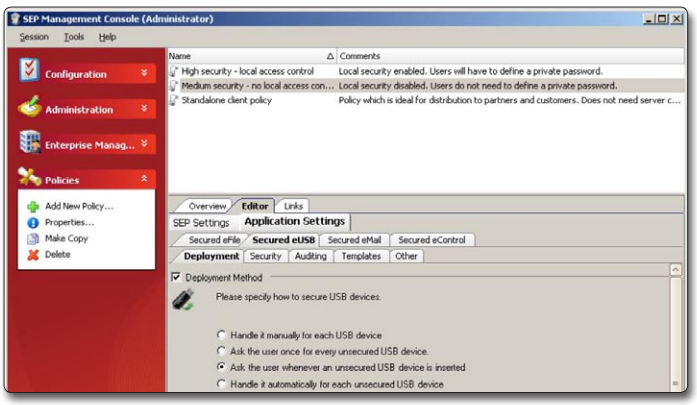


Figura 1. Console de Administração do Cryptzone (SEP)

Apesar da quantidade diversificada de soluções para a proteção básica de notebooks, podemos utilizar o Secured eDisk para ter uma proteção completa de todo o disco fixo presente em desktops, servidores e notebooks, assim como em mídias removíveis. O que o difere de outros módulos específicos são algumas funcionalidades que complementam a gestão, incluindo monitoramento do uso dos dispositivos e outras funções avançadas.

Entre suas principais características, destacamos a opção de Single-Sign-On, que permite ao usuário a inserção de seus dados de login uma única vez em uma tela que é carregada no processo de pré-boot, conforme o exemplo mostrado na **Figura 2**. Neste momento a conta do usuário é autenticada com a confirmação da senha e domínio da rede, permitindo o acesso direto ao sistema Windows.



Figura 2. Tela de autenticação pré-boot com Single-Sign-On

Outra funcionalidade muito importante e usada nas corporações é o bloqueio de tentativas de acesso que pode ser configurado pelo administrador responsável. Neste caso, ao realizar, por exemplo, três tentativas sem sucesso, a autenticação ficará bloqueada por um tempo determinado, com uma mensagem similar à apresentada na **Figura 3**.



Figura 3. Aviso de bloqueio de acesso pelos próximos 3 minutos

Se realmente o usuário tiver esquecido a sua senha de acesso ou, ainda, se o notebook foi transferido a outro funcionário que não possua a senha de seu antigo proprietário, este pode solicitar à equipe de suporte da organização que libere uma nova senha de acesso.

Para isso, o usuário devidamente identificado e autorizado pelo suporte técnico da organização deverá informar o código exibido na tela que é gerado pela própria ferramenta ao apertar a combinação de teclas [Shift + F10]. Um exemplo da tela de recuperação pode ser vista na **Figura 4**.



Figura 4. Código usado no Console de Administração para gerar a Contra-Chave

Com este código, o administrador do Console do Cryptzone poderá identificar o equipamento e gerar uma Contra-Chave para liberar um acesso emergencial ao sistema, permitindo assim que o usuário possa realizar a troca da senha, conforme a **Figura 5**.

Caso o notebook seja extraviado, as informações não estarão disponíveis, mesmo que o intruso tente conectar o disco em outro computador para realizar a leitura. O mesmo tipo de proteção pode ser preparado para mídias removíveis. Na **Figura 6** temos um exemplo de como é simples criptografar dispositivos removíveis, apenas clicando com o botão direito do mouse.



Figura 5. Substituição da senha realizada diretamente no Windows

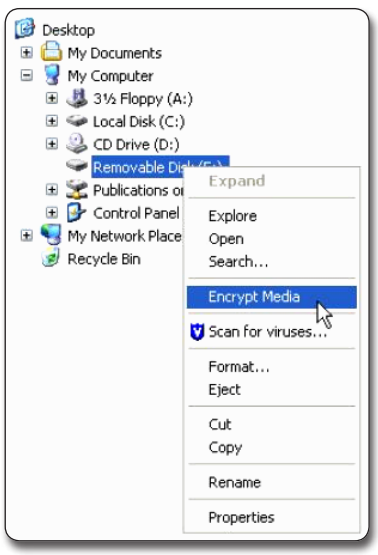


Figura 6. Criptografando uma unidade de disco removível

Realizada a encriptação do dispositivo removível, o Cryptzone cria um executável que permite a abertura do "cofre" criado em qualquer computador, mesmo que este não possua uma licença da solução instalada. Para ter acesso aos dados armazenados no dispositivo, o usuário deverá clicar duas vezes no ícone do arquivo executável, como exibido na **Figura 7**. Com isso será preciso apenas inserir a senha definida durante o processo de criptografia. Sem esta senha é praticamente impossível o acesso ao conteúdo protegido. Por este motivo, caso a tenha esquecido, o usuário poderá recuperá-la clicando na opção "Click here if you have lost your password", solicitando ao administrador uma nova senha conforme mostrado na **Figura 8**.

Além disso, a solução Cryptzone permite trabalhar em conjunto com outros dispositivos de autenticação, como leitores biométricos e tokens, complementando assim a segurança no acesso dos dispositivos. Na **Figura 9** temos um exemplo de autenticação combinada.

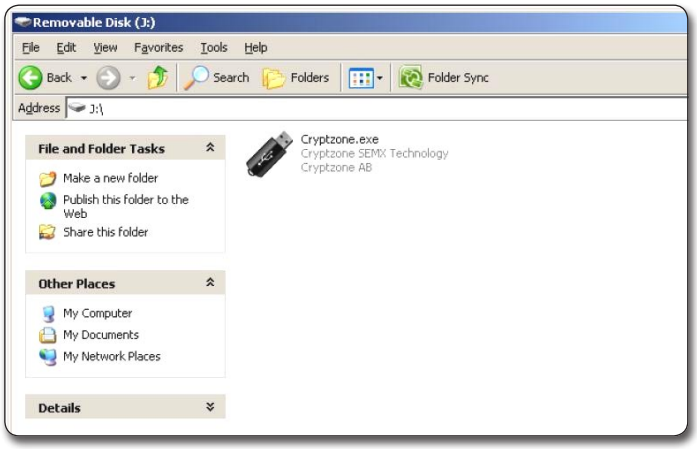


Figura 7. Criptografando uma unidade de disco removível



Figura 8. Criptografando uma unidade de disco removível



Figura 9. Tela de logon do Windows com Cryptzone e opção de inserção de token

TrueCrypt

Como já falamos, TrueCrypt é um programa Open Source com a finalidade de criar e manter uma unidade de armazenamento de dados, fixa ou removível, criptografada. Mesmo sendo uma opção gratuita, não deixa nada a dever em relação aos grandes players do mercado no quesito criptografia. Como já mencionado anteriormente, sua maior limitação é quanto ao seu gerenciamento local, que pode ficar inviável quando se tratando de uma empresa com diversos dispositivos móveis.

O TrueCrypt pode criptografar toda a partição de um disco ou criar volumes que são montados como unidades virtuais (containers). Veja na **Figura 10** estas opções. Seu processo de criptografia é transparente e realizada em tempo real on-the-fly (ver **Nota DevMan 1**).

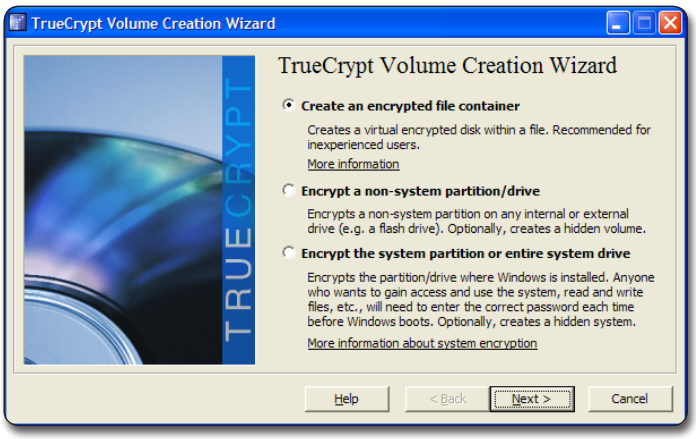


Figura 10. Opções de criptografia da solução TrueCrypt



Nota do DevMan 1

On-the-fly: O termo on-the-fly significa que os dados armazenados na unidade são automaticamente criptografados ou descriptografados antes de serem abertos ou fechados, sem qualquer intervenção do usuário.

Trata-se de um software robusto na questão da proteção efetiva dos dados e que gera muita dor de cabeça para os peritos que trabalham na coleta de evidências em investigações de crimes digitais, em razão da impossibilidade de acesso às informações sem a inserção da senha cadastrada, que é exatamente o caso do banqueiro Daniel Dantas. Veja algumas de suas características técnicas:

- Compatível com sistemas Windows, Linux e Mac OS;
- Criptografia automática, em tempo real (on-the-fly), transparente para o usuário;
- Cria um disco virtual criptografado dentro de um arquivo;
- Criptografa partição de dispositivo de armazenamento móvel (pen drives, HDs externos);
- Criptografa todo o disco, incluindo sistemas operacionais Windows (pré-boot);
- Utiliza os algoritmos de criptografia: AES-256, Serpent e Twofish (**Figura 11**).

Criando um container, o usuário poderá criar uma unidade de disco virtualizada dentro de uma unidade de disco lógica que pode ser transportada de um dispositivo a outro, garantindo a inviolabilidade das informações presentes neste container. Sendo assim, podemos, por exemplo, criar um container chamado "My Volume" dentro da pasta Meus Documentos (**Figura 12**) num computador com o tamanho de armazenamento de 1 GB para armazenar somente arquivos importantes e sigilosos.

O usuário pode definir o tamanho do container de acordo com o espaço que ele possui no disco físico e de acordo com o tipo de partição utilizada. Se a partição for do tipo FAT32, o limite será de 4GB por container, pois é o tamanho máximo de alocação que este

tipo de partição suporta. Caso a partição seja NTFS, este tamanho vai variar de acordo com o tamanho do volume, o que na teoria é ilimitado, conforme aumentam o tamanho dos discos rígidos.

Na **Figura 12** acessamos o container criptografado com a solução TrueCrypt, que imediatamente solicita a escolha de uma unidade para montar o container e a inserção da senha de acesso para sua abertura na unidade selecionada, que no exemplo da **Figura 13** é a unidade M:\.

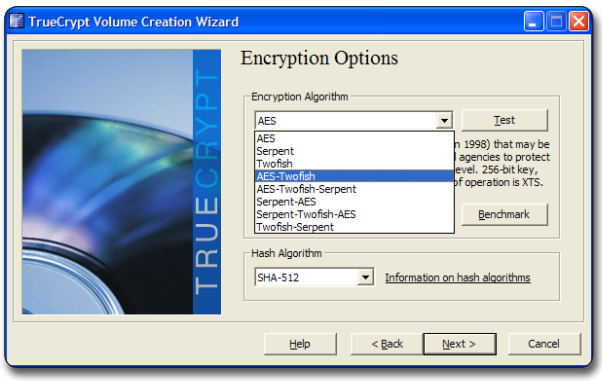


Figura 11. Algoritmos de criptografia disponíveis para proteção

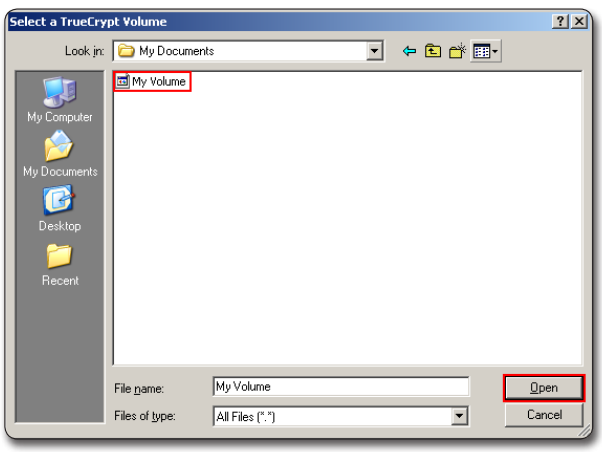


Figura 12. Acessando o container criptografado "My Volume"

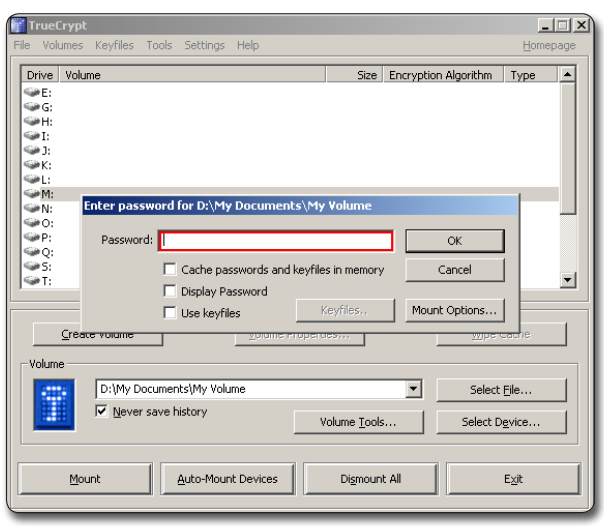


Figura 13. Senha para abertura do container "My Volume"

Agora temos o container montado na unidade M:\ (**Figura 14**). Assim, todos os arquivos armazenados de forma segura dentro de "My Volume" estarão disponíveis na unidade virtual M:\ com 1 GB de espaço disponível.

Ao acessar o Meu Computador (**Figura 15**), temos uma nova unidade de disco criada, permitindo o acesso destes arquivos até o fechamento do TrueCrypt, que fechará a unidade, protegendo todos os arquivos dentro do container especificado.

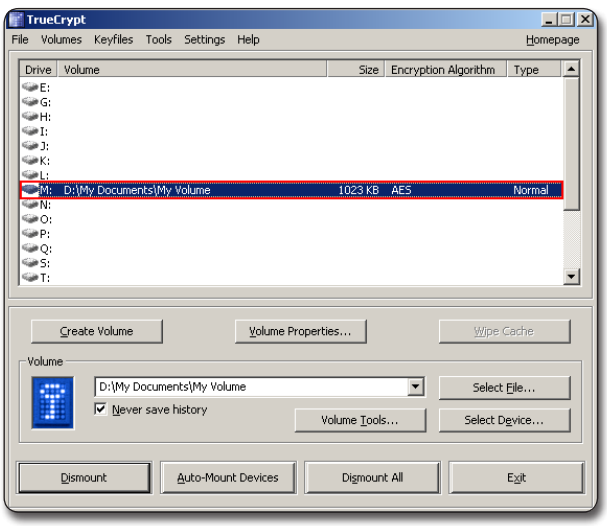


Figura 14. Container "My Volume" montado na unidade M:\ com 1 GB de espaço

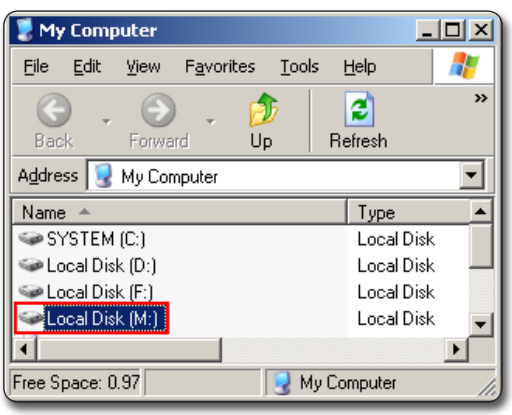


Figura 15. Container "My Volume" montado na unidade M:\

Um detalhe importante: todo conteúdo presente em "My Volume" que o usuário criou com o TrueCrypt só poderá ser aberto em computadores que possuam a solução instalada, obviamente com a inserção da senha de acesso.

Outra opção muito utilizada por quem faz uso do TrueCrypt é a criptografia de toda a partição do disco. Peguemos como exemplo o caso de roubo ou extravio de um notebook. Com este tipo de criptografia, o notebook somente terá alguma utilidade se for apagada toda a partição e tudo for reinstalado do zero, garantindo assim a confidencialidade de todo o conteúdo.

Quando o notebook está com todo o disco criptografado, o acesso ao sistema operacional só será possível depois de inserida a senha de acesso na tela de pré-boot, conforme apresentado na **Figura 16**.



Figura 16. Tela exibida no pré-boot do sistema operacional criptografado com TrueCrypt

Diferentemente do Cryptzone, que oferece uma possibilidade de recuperação da senha por meio da gestão do Console Central, o TrueCrypt não oferece ao usuário este tipo de Recovery. Isso é muito complicado em situações de desligamento de funcionários da empresa, pois se ele não informar a senha de acesso do notebook ao seu superior ou ao departamento de TI, não haverá outra opção a não ser formatar o disco para ter o equipamento operacional novamente.

Outra situação muito comum é o esquecimento da senha por parte do usuário. Neste caso, se não houver backup, além do tempo de reinstalação, perde-se todo o material de trabalho armazenado.

Por essas razões, o uso deste tipo de software open source é recomendado para usuários domésticos. Neste caso é necessário ter um disco de recuperação com uma senha mestra para cada computador. Assim, caso a senha seja esquecida, basta inserir a mídia de recuperação com a senha mestra para obter acesso novamente aos dados criptografados, como mostra a **Figura 17**.

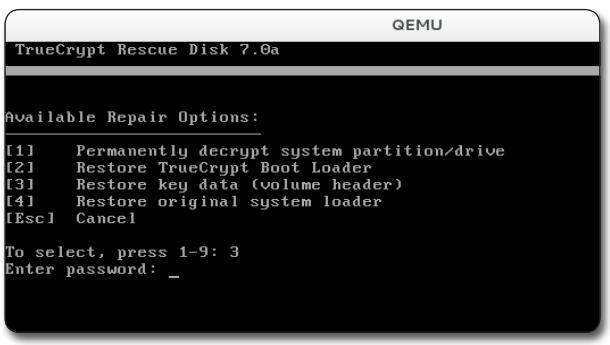


Figura 17. Tela de recuperação do TrueCrypt

Fazer esta gestão de mídias de recuperação em um notebook até é possível, mas em um ambiente corporativo com vários equipamentos, torna-se uma tarefa inviável.

Outro diferencial importante que faz bastante falta em um ambiente corporativo é o recurso Single-Sign-On. No TrueCrypt, não há essa integração que facilita e muito a gestão das senhas de acesso dos usuários.

Conclusão

Lendo este artigo podemos chegar a inúmeras conclusões. Podemos observar que o crescimento do uso de dispositivos móveis impacta diretamente no aumento do número de incidentes de segurança que envolva perda e vazamento de informações confidenciais, o que pode afetar negativamente tanto o negócio como a vida profissional e pessoal de qualquer um de nós.

Também podemos notar que por mais antigo e conhecido seja o conceito de criptografia como forma de proteção contra vazamento de informações e acessos não autorizados, sua adesão ainda é extremamente baixa se compararmos com o nível de avanço tecnológico que está hoje ao alcance de todos nós, mortais.

E, por fim, podemos concluir que há soluções para todos os dispositivos móveis, tanto para grandes ambientes corporativos como para o simples usuário doméstico. Há opções de soluções pagas, com todos os recursos e suporte técnico, assim como soluções gratuitas, suportadas pela comunidade de desenvolvedores na Internet.

Mas a principal lição que os leitores podem levar desse estudo é que, por mais valioso que pareça, qualquer equipamento pode ser substituído fisicamente por outro igual ou, às vezes, até por outro melhor. No entanto, as suas informações, essas são únicas e em muitos casos, de valor inestimável.

Dando um exemplo bastante absurdo, o que você acha que é mais importante para uma empresa como a fabricante de bebidas Coca-Cola? Toda sua infraestrutura de TI espalhada pelo mundo ou a sua secreta fórmula que pode estar registrada em "um papel de pão"?



Roberto Henrique de Sousa
roberto@abctec.com.br
É Analista de Segurança da Informação na ABCTec, com 14 anos de experiência na área de TI (Suporte, Gestão, Consultoria), especializado em análise de vulnerabilidades e no tratamento de incidentes de segurança da informação. Formado em Análise e Desenvolvimento de Sistemas, possui as certificações ISFS ISO/IEC 27002 Certified, F-Secure Certified Technical Professional - FSCTP, D-Link DBC, Microsoft MCP/MCDST.

Site da Cryptzone
http://www.cryptzone.com

Site da TrueCrypt
http://www.truecrypt.org

Rede Nacional de Ensino e Pesquisa – Curso Introdutório ao uso de PGP
http://www.rnp.br/_arquivo/documentos/ref0181.pdf

Cartilha de Segurança para Internet - CERT
http://cartilha.cert.br

Blog do autor
http://abctec.blogspot.com

SSH – Protocolo seguro para acesso remoto

Utilizando SSH e um protocolo Cliente/Servidor para transmissão criptografada de dados na rede

Atualmente a maioria das empresas hospeda seus serviços e aplicações de banco de dados fora de suas recem toda instalação e segurança necessárias, com as devidas redundâncias, para sempre manter os serviços executando de forma confiável.

Neste cenário, é natural que você queira fazer conexões remotas nesses servidores para alteração de configuração de algum serviço ou aplicação, atualização de segurança, instalação de algum serviço adicional, copiar arquivos do seu computador para o servidor ou vice-versa. Para executar todos esses passos temos diversas ferramentas como FTP, RCP, Telnet, Rlogin, RSH, SSH entre outros.

Infelizmente, muitos desses programas relacionados a acesso remoto têm um problema fundamental, eles não possuem segurança eficaz. Na tentativa de transmitir um arquivo confidencial através da rede, um intruso pode parcialmente interceptar os dados utilizando ferramentas de sniffer e lê-los (ler **Nota do DevMan 1**). Um exemplo deste problema pode ser encontrado na utilização do Telnet (ler **Nota do DevMan 2**). Este protocolo não aplica criptografia nos dados transmitidos, o que deixa sua comunicação exposta na rede.

Na **Figura 1** temos um exemplo do wireshark, uma ferramenta de sniffer de rede capturando dados de uma comunicação realizada com Telnet. Podemos perceber que nos dados transmitidos nessa comunicação não são aplicados hash de criptografia, o que torna fácil identificar os dados transmitidos na comunicação.

Para amenizar esses problemas você pode utilizar um Firewall que proteja os computadores da rede de um intruso, pode utilizar hash de comunicação para embaralhar os dados tornando sua leitura impossível, ou utilizar o SSH. O SSH é uma ferramenta com ênfase em segurança que utiliza um conjunto de técnicas de criptografia para assegurar que apenas a pessoa autorizada possa conectar ao servidor e que todos os dados transmitidos sejam impossíveis de decifrar mantendo, dessa forma, a integridade da conexão. A ferramenta possui diversas respostas a ataques conhecidos. Por exemplo: o SSH detecta casos em que o servidor tenha sido trocado por outro; situações nas quais se tenta injetar dados na conexão (tirar proveito de uma conexão aberta para incluir pacotes na conexão, alterando as informações passadas); e técnicas de ocultação de pacotes, o

Resumo DevMan

De que se trata o artigo:

Neste artigo serão apresentadas as principais características do protocolo SSH, bem como as novas instalações, configurações e customizações introduzidas em seu arquivo de configuração. Serão descritos os diferentes tipos de opções e seus parâmetros padrão. Além disso, serão apresentadas algumas mudanças que podem ocasionar melhor desempenho e melhor segurança dependendo do ambiente de produção onde se encontra instalada a ferramenta SSH. Por fim, serão expostas as técnicas de túneis criptográficos, e a utilização de chaves simétricas e assimétricas.

Em que situação o tema é útil:

Os pontos destacados neste artigo serão úteis para a compreensão do protocolo SSH, bem como de suas principais diferenças quando comparado a outras ferramentas de conexão remota. Os conceitos expostos também permitirão o aprofundamento técnico do tema pelos profissionais e usuários da área de infraestrutura de tecnologia da informação.

SSH – Protocolo seguro para acesso remoto:

Inicialmente apresentaremos uma introdução ao tema segurança de dados. Em seguida, apresentaremos a ferramenta SSH, com o objetivo de entendermos como podemos obter uma transmissão segura de dados em nossa rede. O artigo abordará também a instalação, configuração e customização da ferramenta SSH.

que torna mais difícil descobrir em qual pacote criptografado foi transmitida a senha.

Neste contexto, para tentarmos obter uma transmissão segura dos dados em nossa rede, abordaremos a partir de agora a instalação, configuração e customização da ferramenta SSH. Esta possui grande eficiência em termos de segurança na transmissão de dados e comunicação remota.



Nota do DevMan 1

Sniffer: Sniffer (analisador de pacote de rede) é uma ferramenta capaz de interceptar e registrar o tráfego de dados em uma rede de computadores. À medida que os dados trafegam na rede, o sniffer captura os pacotes e os decodifica.



Nota do DevMan 2

Telnet: Telnet é um protocolo de conexão remota que permite a comunicação de terminais e de aplicações através da internet.

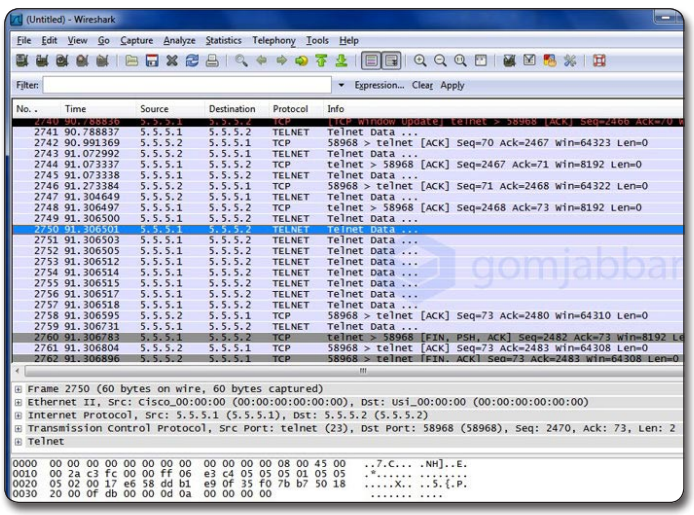


Figura 1. Capturando dados de comunicação Telnet

O que é SSH?

Desenvolvido por Tatu Ylonen em 1995 para uso no Unix, o SSH (Secure Shell) é uma ferramenta de acesso remoto com grande ênfase em segurança. Com o SSH, sempre que os dados forem enviados de uma máquina para outra, os dados enviados de host a host serão automaticamente criptografados e descriptografado (trata-se de uma criptografia transparente).

Caso você tenha alguma desconfiança sobre algoritmos de criptografia (por exemplo, se os mesmos podem ser quebrados com força bruta), considere a seguinte situação que demonstra como o algoritmo utilizado pelo SSH é confiável: uma chave de 64 bits que era utilizada no SSL dos navegadores necessitaria de um cluster de 250 servidores Xeon para quebrar a senha, que é 16 milhões de vezes mais forte que uma de 40 bits utilizada em protocolos WEP. Já a chave de 128 bits é 19.567.000.000.000.000.000 vezes mais forte que uma chave de 64 bits, o que tornaria o processo muito demorado. Um servidor SSH bem configurado é de certa forma impenetrável e você pode utilizá-lo de forma segura mesmo se sua rede estiver comprometida.

O SSH utiliza um conjunto de algoritmos de criptografa moderno e seguro para permitir a transmissão confiável de dados em sua conexão, mantendo assim a integridade das informações transmitidas. Sua arquitetura cliente/servidor, normalmente instalada e executada por um administrador de sistema, pode utilizar o SSH para aceitar e rejeitar conexões de entrada para seu host, limitando os IPs ou o range de IPs que poderão iniciar a conexão com o servidor SSH.

A **Figura 2** apresenta um modelo cliente/servidor de uma conexão SSH onde os hosts com permissão de iniciar a conexão conseguiram acesso e os hosts sem permissão tiveram a conexão bloqueada pelo servidor SSH.

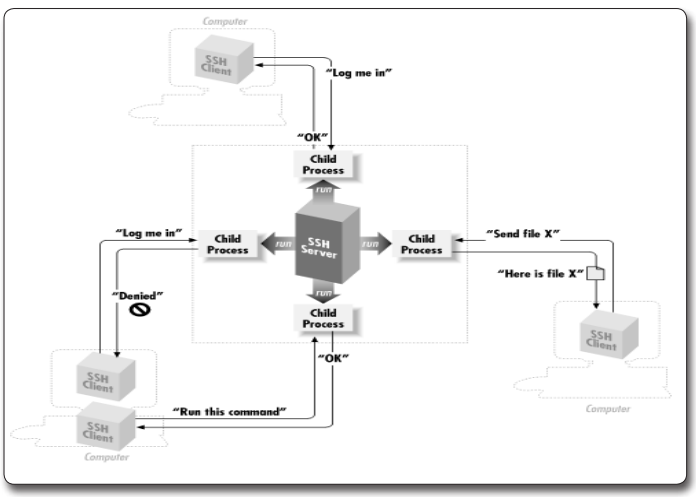


Figura 2. Comunicação Cliente/Servidor do Protocolo SSH

O SSH utiliza um conjunto de criptografia de chaves assimétricas onde, além de uma chave pública que permite que todos possam criptografar os dados, existe uma chave privada que apenas as máquinas que irão fazer a conexão possuem para poder descriptografar os dados. Quando o usuário se conecta a um servidor SSH, seu host e os servidores trocam suas chaves públicas, permitindo que um envie informações para o outro de forma segura. É através deste canal que é feita a autenticação, seja ela por login e senha, seja utilizando uma chave e passphrase.

O SSH realiza a conexão entre o cliente e o servidor sempre utilizando chaves de 512 bits. Desta forma, é praticamente impossível quebrar este nível de criptografia. Entretanto, ele demanda um grande volume de processamento, e se o SSH transmitisse toda informação com esse algoritmo, sua comunicação ficaria muito lenta. Para resolver esse problema, depois de ter feito a autenticação, o SSH utiliza um algoritmo mais simples para

transmitir os dados entre o cliente e o servidor. Este algoritmo mais simples demanda menos processamento para transmitir os dados, tornando a comunicação mais eficiente.

Na **Figura 3** temos um exemplo de um túnel SSH encriptado, onde cliente e servidor realizam a autenticação para transmissão dos dados.

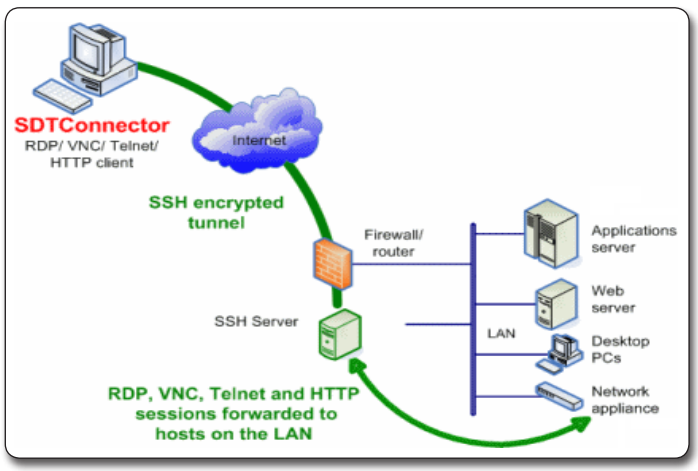


Figura 3. Túnel encriptado na comunicação do protocolo SSH

O SSH é dividido em dois módulos:

- sshd: é o daemon (script para inicialização ou parada de um serviço) do serviço do protocolo SSH, e fica residente no servidor;
- ssh: é apenas uma aplicação instalada no cliente para fornecer uma interface de comunicação com o servidor.

Para instalar o SSH em um servidor derivado de distribuição Debian, devemos executar o seguinte comando no terminal:

```
# apt-get install openssh-server
```

Para realizar a mesma instalação utilizando uma distribuição derivada da família Red Hat, executamos o mesmo comando, trocando apenas o gerenciador de instalação para o da família Red Hat:

```
# yum install openssh-server
```

Feita a instalação em modo servidor, o serviço do SSH já é iniciado automaticamente durante o boot, mas caso tenha algum problema e o daemon não seja iniciado automaticamente, você poderá iniciá-lo da seguinte forma:

- Debian:

```
#/etc/init.d/sshd start
```

- Red Hat:

```
# service sshd start
```

O SSH utiliza a porta 22 para se conectar, havendo a possibilidade de alterá-la (mas não entraremos nesse detalhe). Por conta disso, é necessário manter a porta 22 no firewall aberta, pois o protocolo SSH utiliza essa porta para comunicação, e caso a porta esteja fechada, a comunicação será filtrada ou negada pelo firewall.

Concluída a instalação do servidor SSH que irá disponibilizar o serviço necessário para comunicação, é preciso instalar o cliente SSH. Este é a ferramenta utilizada para efetuar a comunicação com o servidor. O pacote openssh-client é o cliente do SSH utilizado para se comunicar com o servidor.

A configuração do servidor SSH baseado na distribuição Unix-like mantém seu arquivo de configuração em /etc/ssh/sshd_config, e /etc/ssh/ssh_config para o pacote instalado no cliente.

Configuração do servidor SSH

É possível alterar diversas opções relacionadas ao servidor SSH, bastando apenas editar o arquivo /etc/ssh/sshd_config. Alguns exemplos de configuração são: a porta de comunicação, a lista de IPs que o protocolo irá permitir conectar, a versão do protocolo a ser utilizada e os usuários que poderão se conectar ao servidor SSH.

Os arquivos de configuração do servidor e do cliente SSH já vêm com configurações padrão da porta de comunicação, versão do protocolo SSH a ser utilizada e a lista de IPs que poderão se conectar no servidor SSH. Isto possibilita que eles já possuam uma segurança razoável. Entretanto, é sempre necessário alterar as opções do arquivo de configuração do servidor SSH de acordo com a necessidade da empresa, trazendo uma tranquilidade maior e evitando qualquer tipo de incômodo que possa ocorrer por causa de um intruso.

Conheceremos a partir de agora algumas das principais opções relacionadas ao arquivo de configuração do servidor SSH.

Porta

Esta é a primeira linha do arquivo de configuração do servidor SSH. Como já mencionado, a porta padrão de comunicação é a de número 22.

Algumas empresas adotam um padrão mais rigoroso de segurança e alteram essa porta para uma porta acima de 1024, pois a maioria dos scanners de portas é baseada em assinaturas de portas já conhecidas, ou seja, serviços que por padrão definem uma porta para execução. Dessa forma será dificultada a identificação do serviço que está em execução na porta do servidor. Portanto, ao conectar com o cliente no servidor SSH, é necessário usar a opção -p no cliente para indicar a porta de conexão. Por exemplo:

```
# ssh -p 2229 fandezhi.efglobe.com
```

Outra forma de se comunicar com o servidor SSH em uma porta diferente da padrão é alterar o arquivo de configuração do cliente SSH e alterar o campo Port para a porta utilizada pelo servidor SSH. Esse tipo de técnica vem sendo utilizada porque a maioria dos ataques já faz rastreamento em portas padrões de serviços

como 21, 22, 23 e 80. Alterar a porta para uma mais alta deixa o servidor menos exposto.

Lista de Acesso

Logo abaixo da opção de porta no arquivo de configuração do servidor SSH, temos a opção que define a interface de rede ou IP que poderá requisitar o servidor SSH sem a necessidade de um firewall. Para exemplificar, considere um servidor SSH que rode no endereço 192.168.1.1 e você quer apenas liberar o acesso ao servidor para esse intervalo de IP. Para isso, será necessário definir a seguinte informação no arquivo de configuração:

```
ListenAddress 192.168.1.1
```

Perceba que foi necessário informar apenas o endereço IP da máquina onde o SSH roda, e não a lista de endereços completa da rede.

Protocolo

O SSH é utilizado atualmente na versão SSH2, mas alguns clientes ainda rodam o serviço na primeira versão. No campo protocol você pode especificar de quais versões o SSH irá aceitar conexões, por exemplo:

```
Protocol 2,1
```

Por questão de segurança é sempre bom deixar o SSH 1 desativado, o que neste caso iria alterar a linha no arquivo de configuração para:

```
Protocol 2
```

Usuários e Senhas

Uma das opções que podemos utilizar para o login é a seguinte:

```
PermitRootLogin no
```

Esse campo irá bloquear a conexão direta como usuário root. Esse é um parâmetro de segurança, pois o usuário terá que logar como um usuário normal, sem privilégios, e depois terá que invocar o su para se tornar root, podendo então fazer qualquer alteração no sistema. Para permitir logar diretamente como usuário root, basta alterar o campo para:

```
PermitRootLogin yes
```

Outra forma é restringir os usuários do sistema que poderão logar no servidor SSH, utilizando o seguinte parâmetro (colocando os nomes separados por espaço):

```
AllowUsers sotam fire
```

Ou negar os usuários que não poderão logar no servidor SSH:

```
DenyUsers beta teta
```

Outra opção muito utilizada é a de não permitir o usuário logar se sua senha estiver vazia. Essa restrição pode ser definida da seguinte forma:

```
PermitEmptyPasswords no
```

Banner

O banner é a opção utilizada para mostrar uma mensagem de aviso ou advertência no momento em que o prompt do terminal loga no servidor SSH. Você pode especificar esse parâmetro da seguinte forma:

```
Banner = /etc/issue.net
```

X11

Esta é uma opção utilizada para clientes que desejam executar aplicativos gráficos. Ela pode ser definida da seguinte forma:

```
X11Forwarding yes
```

Configuração do cliente SSH

Quando instalado, o SSH permite que todas as contas cadastradas no sistema façam conexão remota na máquina. Assim, para se conectar a uma máquina com IP 192.168.10.1 usando o padrão normal de conexão, teríamos:

```
# ssh zukiari@192.168.10.1
```

Você também pode utilizar a opção –l, que representa o login do usuário para conexão da seguinte forma:

```
# ssh -l zukiari 192.168.10.1
```

Além disso, você pode conectar a uma máquina em uma mesma rede apenas chamando seu nome, como em ssh zukiari@, e, caso omitido o usuário na conexão, o SSH utiliza o próprio usuário logado na máquina para tentar a conexão.

Conexões SSH que necessitem rodar aplicativos gráficos podem utilizar a opção –X. Esta irá habilitar a execução de janelas gráficas "Xterm" para a inicialização do aplicativo, ou você pode adicionar ou remover o comentário da opção "X11Forwarding = yes" do arquivo de configuração do cliente SSH.

Tempo de Execução

O SSH, por padrão, mantém um tempo de ociosidade de cada usuário e o desconecta caso ele fique sem interagir com o terminal de acesso remoto um tempo maior que o definido no arquivo de configuração. Isto pode se tornar um incômodo quando estamos trabalhando nos terminais e precisamos sempre digitar alguma informação para que não sejamos desconectados.

Para evitar esse trabalho, podemos adicionar um parâmetro que irá permitir que o cliente permaneça enviando pacotes para o servidor, mantendo desta forma a conexão aberta.

Para ativar esse recurso, adicione a seguinte linha no final do arquivo SSH ou em qualquer parte do arquivo, especificando o tempo em segundos para manter a conexão aberta:

```
ServerAliveInterval 120
```

Parâmetros de autenticação com chaves

Diante da existência da possibilidade de um invasor conseguir descobrir sua senha, o SSH oferece um tipo de autenticação baseado em duas chaves. Isto melhora o nível de segurança, pois desta forma não dependemos apenas de uma senha para o login. Ao invés disso, teremos duas chaves: uma chave pública instalada no servidor SSH, e uma chave privada protegida por um passphrase. Com estas duas chaves será necessário saber o passphrase para estabelecer a conexão e ainda ter a chave privada instalada em seu computador. Sem essa chave é impossível fazer a conexão. Dessa forma, teremos uma segurança de dois níveis, onde é preciso saber o passphrase e ter a chave privada dentro do computador (ou qualquer meio de armazenamento). Para gerar essas chaves (cliente), usamos o seguinte comando:

```
# ssh-keygen -t rsa
```

A saída para esse comando pode ser vista na **Listagem 1**.

Listagem 1. Saída do comando de geração de chave.

```
Generating public/private rsa key pair.

Enter file in which to save the key (/zukiari/.ssh/id_rsa):

Created directory '/zukiari/.ssh'.

Enter passphrase (empty for no passphrase):
********* ********* ********* ********* *********
Enter same passphrase again:
********* ********* ********* ********* *********
Your identification has been saved in /zukiari/.ssh/id_rsa.

Your public key has been saved in /zukiari/.ssh/id_rsa.pub.

The key fingerprint is:

4e:0c:3d:fb:7d:d8:be:e5:5f:09:e2:10:9e:d6:a8:e0 zukiari@kelevra
```

Este comando irá gerar os arquivos .ssh/id_rsa e .ssh/id_rsa.pub dentro do diretório do usuário que o executou. É aconselhável não utilizar o root para executar esse comando, mas sim o usuário que você utiliza para se conectar ao servidor SSH. Os arquivos gerados são respectivamente uma chave privada e uma chave pública.

O arquivo .ssh/id_rsa é um arquivo oculto e sua permissão de acesso deve ser alterada para 600, de forma a evitar o acesso do arquivo por outros usuários (alguns servidores proíbem a conexão se o arquivo estiver com permissões incorretas). Gerado o par de chaves, agora é necessário instalar a chave no servidor para que ele entenda e permita a autenticação:

```
# ssh-copy-id -i ~/.ssh/id_rsa.pub zukiari@serve
```

O comando ssh-copy-id irá copiar a chave pública gerada para o servidor e irá instalá-la no servidor. Feito isso, ao tentar logar no servidor SSH não será necessária mais a senha. O servidor irá enviar um "teste" encriptado usando a chave pública compartilhada. Para respondê-lo, o cliente SSH irá precisar de uma chave privada, que precisa de um passphrase para destravá-la.

A instalação manual dessa chave também é possível da seguinte forma: o arquivo .ssh/id_rsa.pub é composto por uma única linha muito longa que contém sua chave pública de encriptação. Ela possui o seguinte formato:

```
# ssh-rsa 2yVe4cBNMz5LZj7fNvaoNiYbrfgwWbD/SzfSwMMWSMYZJV4yXQmK9
```

Você pode conectar no servidor SSH e copiar a linha para dentro do arquivo .ssh/authorized_keys. Isto pode ser feito usando qualquer editor de texto normal. Assim, o final do arquivo .ssh/authorized_keys do servidor SSH terá o mesmo conteúdo do arquivo .ssh/id_rsa.pub da máquina cliente, o que irá fazer o servidor remoto passar a verificar a sua chave privada com o passphrase ao invés da senha.

Dessa forma, você pode incrementar a segurança do SSH proibindo a conexão no servidor com qualquer tipo de senha, mesmo a do root, apenas habilitando o uso dos pares de chaves. Para executar esse tipo de configuração, você terá que alterar o arquivo de configuração do servidor SSH (/etc/ssh/sshd_config) modificando ou inserindo as seguintes opções:

```
PasswordAuthentication no
UsePAM no
```

O parâmetro PasswordAuthentication no irá desativar o uso de senhas e o UsePAM no desativa qualquer tipo de autenticação exceto por chaves. Em seguida, é necessário reiniciar o serviço do SSH para que as alterações entrem em vigor. Para isso, você pode proceder da seguinte forma:

```
# /etc/init.d/sshd force-reload
```

ou:

```
# service sshd force-reload
```

Existe também a possibilidade de se utilizar múltiplas chaves, ou seja, um passphrase para cada conexão que existir. Imagine que você tenha 20 servidores. Dessa forma você teria 1 passphrase para cada servidor, e não somente um passphrase para todas as conexões. Esse é um parâmetro de segurança exigido, pois se um invasor descobrir um passphrase para um servidor, terá que descobrir outro passphrase para a outra conexão. Para gerar novas chaves, use o comando ssh-keygen -t rsa, apenas prestando atenção para alterar o diretório onde você deseja salvar as chaves.

Desta forma você pode gerar quantos pares quiser e, antes da comunicação, basta utilizar o ssh-copy-id com a opção -i e

especificar o caminho até a chave mais o servidor para conexão, como no exemplo:

```
# ssh-copy-id -i /zukiari/.ssh/id_rsa zukiari@serve
```

Logins automáticos com o SSH

Esta é uma opção muito utilizada por administradores de redes. Não é incomum termos que administrar mais de 20 servidores, o que acaba se tornando cansativo e monótono por conta da repetição do login a cada conexão. Uma forma de amenizar este problema é o uso do login automático. Isto pode ser feito de duas formas.

A primeira é deixar o passphrase vazio e apenas autenticar com a identificação da chave privada. Entretanto, essa é uma opção não muito utilizada por motivos de segurança, pois se alguém, de alguma forma, conseguir sua chave privada (alguém consegue acesso físico ao seu computador, copia a chave e a coloca em outra máquina), todo seu mecanismo de segurança se tornará inválido. A segunda opção é deixar que o ssh-agent grave seu passphrase na memória em uma área especial, acessível somente pelo ssh-agent. Para utilizar o ssh-agent, execute os seguintes comandos:

```
# ssh-agent
# ssh-add
```

Feito isto, ele irá solicitar seu passphrase. Informado o passphrase, o ssh-agent irá gravá-lo na memória e você não precisará mais se preocupar. Nas situações em que você tenha mais de uma chave para autenticação, basta usar o ssh-add com o caminho da chave que irá utilizar, como no exemplo:

```
# ssh-add /zukiari/.ssh_rsa2
```

Transferência de arquivos remotamente

O SSH pode ser considerado um verdadeiro canivete suíço. Além de sua segurança, ele ainda possui diversas ferramentas que podem auxiliar outros serviços. Um deles é o "scp", uma ferramenta que permite transferir arquivos remotamente entre cliente e servidor apenas pela linha de comando. Esta facilidade pode ser executada da seguinte forma:

```
# scp /home/zukiari/teste.zip zukiari@server:/home/teste/Download
```

O scp ainda permite a utilização de alguns parâmetros que irão auxiliar você a transferir o arquivo. Um exemplo é a opção -p. Esta irá preservar as permissões dos arquivos transmitidos. Alguns exemplos destas permissões são: quem pode alterar, ler ou abrir o arquivo. Você também pode utilizar o parâmetro –r. Este faz a cópia recursivamente e é extremamente útil quando precisamos transmitir dados de um diretório inteiro. Considere que você tenha uma pasta com diversas fotos. Sem precisar comprimir, você pode utilizar o parâmetro –r e fazer a cópia de todo diretório. Você pode também utilizar o parâmetro -v (modo verbose) para mostrar o progresso e os arquivos que estão sendo copiados. Por fim, utilize o parâmetro -C para realizar a compressão dos dados e facilitar a transferência dos arquivos. Observe como ficaria nosso comando considerando este cenário:

```
# scp -prvC /home/zukiari/teste.zip zukiari@server:home/teste/Download
```

SSH no Windows

Um exemplo de cliente SSH para o Windows é o PuTTY, que inclui o PSFTP, um cliente para transferir arquivos usando comandos de transferência como: put, get, cd, lcd e pwd. Este aplicativo pode ser baixado em http://www.putty.org/.

A utilização do PuTTY para conexão é bem simples. Quando feito o download, não é necessária uma instalação. Ele é um arquivo executável apenas.

Na **Figura 4** temos um exemplo de como funciona a ferramenta PuTTY dentro do Windows.

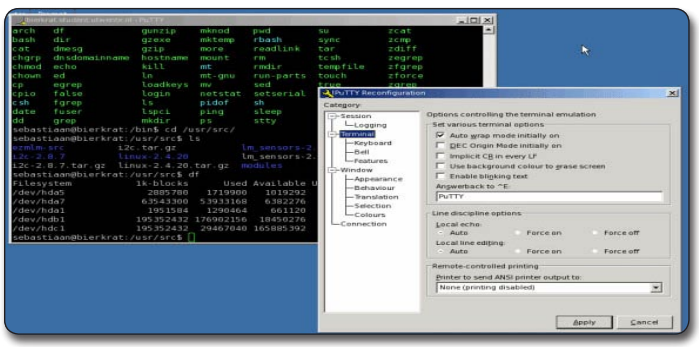


Figura 4. Utilização do PuTTY como ferramenta de conexão remota SSH no Windows

O PuTTY permite diversos tipos de conexões como Telnet, rlogin e SSH, e também trabalha com túneis encriptados. Para iniciar uma conexão, informe o endereço IP ou o domínio do servidor que vai se conectar no campo Host Name (or IP address) na tela principal. Para customização da conexão, utilize os parâmetros do lado direito. Por exemplo: para adicionar um túnel, clique em Connections > SSH > Tunnels, na opção source port defina a porta do seu host que receberá o túnel, e na Destination, defina o endereço IP ou o domínio do servidor seguido da porta, como 192.168.10.1: 2229. Depois é só clicar em open e a conexão remota será iniciada.

Na **Figura 5** temos uma visão geral das opções que a ferramenta PuTTY nos oferece para efetuar conexões remotas e opções para customização da própria ferramenta. Geralmente a conexão é efetuada apenas preenchendo os campo de IP e porta. Feito isso, basta clicar em open e um terminal idêntico ao prompt apresentado na **Figura 4** será visto.

Conclusão

O protocolo SSH, além de ser uma ferramenta segura de conexão remota, possui diversas funções (como firewall interno) que permitem uma proteção bastante abrangente contra ataques tipo

força bruta, DOS, DDOS, transferências de arquivos, execução de ambientes gráficos e túneis seguros. A sua utilização já se tornou padrão e até tecnologias antigas deixaram de ser adotadas, como o Telnet, que foi desativado pela Microsoft nas versões mais recentes do Windows.

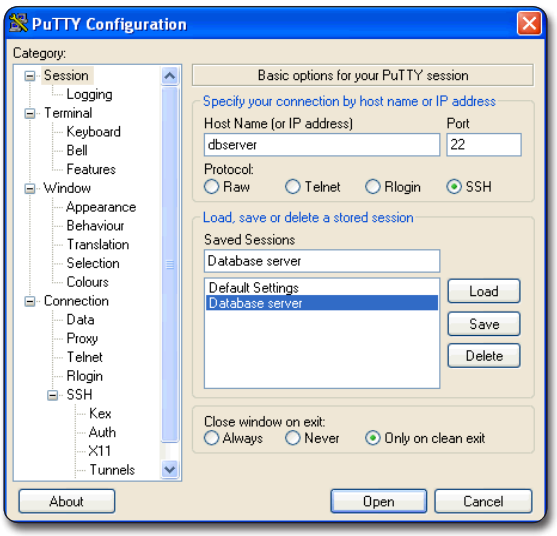


Figura 5. Putty: ferramenta utilizada para acesso remoto via SSH no Windows

Dessa forma, para evitar que seus dados sejam roubados ou sua comunicação ameaçada, uma boa prática é a utilização do protocolo SSH, que lhe traz comodidade quando estiver acessando remotamente servidores para manutenção, transferência de arquivos e instalação de serviços.



Bismarck Matos de Assis

Engenheiro de Redes Cisco, Pós-graduado em Sistemas Distribuídos e Arquitetura Mainframe pela Universidade Latino Americana, especialista em Rede de Computadores e Bacharel em Ciências da Computação pela Faculdade Pitágoras. Atualmente é Engenheiro de Redes no Grupo Fidelity, com ampla experiência na área de redes de computadores e tecnologia da informação com tecnologias Cisco, Juniper Networks, Mikrotiks, Ubiquiti, 3Com, Intelbras. Possui certificações IPv6, FreeBSD SSA, LPI 1, Novell NCLA, CompTia Linux+, NetApp NCDA, Arquitetura Mainframe, 3Com Certified Network Expert e DELL (DCSE).

PuTTY SSH – Cliente de comunicação SSH para Distribuição Microsoft Windows.
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

OpenSSH – Site com informações, atualizações e pacotes para instalação da ferramenta.
http://www.openssh.org/

CURSOS ONLINE

A Revista Java Magazine oferece aos seus assinantes uma série de Cursos Online de alto padrão de qualidade.



CONHEÇA ALGUNS DOS CURSOS:

- Java Básico: Aplicações Desktop
- JSF com Primefaces
- Conhecendo o Apache Struts
- Introdução ao JSP com HTML 5: Intranet Escolar
- Bluetooth: Controle de Aplicação desktop via celular

Para mais informações :
www.devmedia.com.br/curso/javamagazine
(21) 3382-5038

Métricas de segurança

Qual é o nível de segurança da minha organização?

O aumento do número de incidentes de segurança registrados nas redes de comunicações tem trazido preocupação para os profissionais da área e usuários. Os atacantes agem motivados por diferentes razões como buscar notoriedade, obter dados de contas bancárias e cartões de crédito, pressionar grandes corporações ou governos a atenderem suas reivindicações e enfraquecer países inimigos. A rede de jogos online Sony Playstation Network, por exemplo, foi atacada em abril de 2011. Os serviços ficaram indisponíveis por vários dias e dados pessoais dos usuários, incluindo informações sobre cartões de crédito, foram roubados. Em dezembro de 2010, a rede da operadora de cartões de crédito Mastercard foi atacada como retaliação ao bloqueio das doações realizadas ao site WikiLeaks. Os serviços da operadora ficaram indisponíveis devido ao ataque. Em setembro de 2010, o Irã foi atacado pelo vírus Stuxnet, que afetou os sistemas de controle da central nuclear de Bushehr. Suspeita-se que os Estados Unidos e Israel estejam envolvidos no desenvolvimento do vírus, com o objetivo de criar obstáculos ao programa nuclear iraniano. No Brasil, o número de incidentes também tem aumentado, como pode ser observado nas estatísticas apresentadas pelo CERT.br (Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil) na **Figura 1**.

Para proteger os seus ambientes de TI (Tecnologia da Informação), os gestores procuram utilizar ferramentas bastante conhecidas: firewalls, sistemas de detecção de intrusão, servidores de autenticação e autorização, VPN (*Virtual Private Networks*), algoritmos de criptografia, etc. Entretanto, a simples implantação destas ferramentas pode não ser suficiente para garantir que a organização alcançou o nível de segurança desejado. Além de empregar técnicas modernas de segurança da informação, os gestores de TI devem estar aptos a responder perguntas como:

- Os processos de segurança que empregamos são eficientes?
- As medidas de segurança que temos tomado têm trazido melhora à segurança na minha organização?
- O meu ambiente de TI está mais seguro hoje do que era no passado?
- Quais são os pontos nos quais eu devo trabalhar para melhorar a segurança da minha organização?
- Estamos empregando recursos financeiros de maneira eficaz em segurança da informação?

Para que os gestores de TI possam responder estas perguntas de maneira correta, é preciso desenvolver um programa de cálculo e análise de métricas de segurança na organização. Em outras áreas de conhecimento, é comum desenvolver programas de métricas para acompanhar e avaliar a evolução de um segmento.

Resumo DevMan

De que se trata o artigo:

Este artigo apresenta os principais conceitos relacionados às métricas de segurança da informação. Primeiramente, será apresentada a definição de métrica de segurança, juntamente com os principais atributos que uma métrica de segurança deve apresentar. Depois da apresentação destes conceitos iniciais, será apresentado um processo de cálculo e análise de métricas de segurança, que pode ser utilizado na avaliação e na melhoria do nível de segurança de uma organização. Por fim, são apresentados exemplos de métricas de segurança em diferentes áreas como gestão de incidentes, gestão de vulnerabilidades, gestão de mudanças, gestão financeira, infraestrutura de rede e serviços.

Em que situação o tema é útil:

O número de incidentes de segurança tem crescido de maneira alarmante, preocupando as corporações e governos, já que a interrupção de serviços importantes e o roubo de dados sigilosos causa grande prejuízo às organizações. Para que os gestores de TI possam avaliar e melhorar o nível de segurança da informação em suas organizações, é recomendada a utilização de processos de cálculo e análise de métricas de segurança.

Métricas de segurança:

Apesar de haver várias ferramentas no mercado para melhorar o nível de segurança da informação em uma organização, os gestores nem sempre estão confiantes sobre o nível de segurança de sua organização e se os investimentos realizados estão dando o retorno esperado. Para solucionar este tipo de dúvida, os gestores devem adotar processos de cálculo e análise de métricas de segurança. A partir da coleta de dados em todo o ambiente da organização, os gestores podem gerar métricas que ajudarão a avaliar continuamente a evolução do nível de segurança do seu ambiente de TI.

Na Economia, por exemplo, o desenvolvimento econômico de um país é avaliado de acordo com métricas como o PIB (Produto Interno Bruto) e a taxa de desemprego. Ao criar estas métricas, os economistas desenvolveram maneiras objetivas de avaliar a evolução da economia de um país e de comparar diferentes países quanto ao desenvolvimento econômico. Analisando o PIB, é possível determinar quais países tem maior crescimento econômico. Além disso, podemos comparar a situação atual do país com a situação passada, observando se ele melhorou ou não. Na área de segurança de informação, é fundamental que os gestores de TI também possam realizar este tipo de análise em suas organizações.

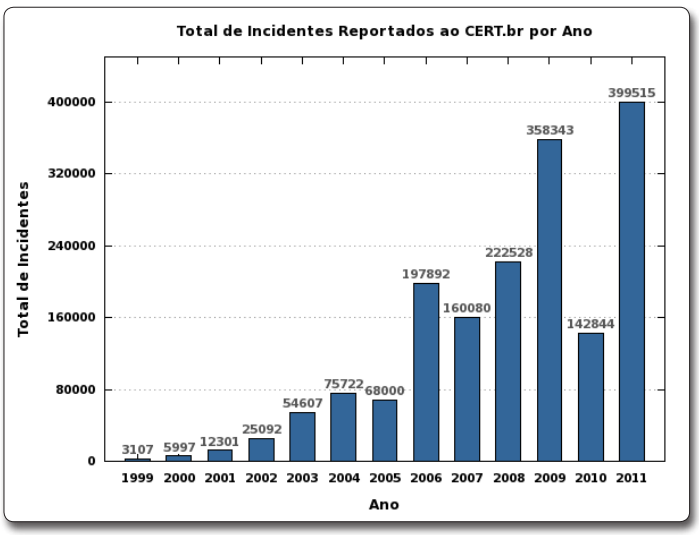


Figura 1. Total anual de incidentes de segurança reportados ao CERT.br (Fonte: http://www.cert.br/stats/incidentes/).

Métricas de Segurança

As métricas de segurança são estabelecidas a partir de análises quantitativas realizadas sobre dados relacionados à segurança da informação coletados em diversos departamentos da organização. A quantidade de computadores com sistema operacional Windows que possuem um software antivírus instalado e atualizado, por exemplo, é um dado relacionado à segurança da informação da organização. Entretanto, o fato de sabermos que existem, por exemplo, 1200 computadores com softwares antivírus corretamente instalados e atualizados não é útil para estabelecer qual é o nível de segurança de informação da organização. Se dividirmos a quantidade de computadores que possuem softwares antivírus pela quantidade total de computadores, passamos a ter uma métrica que é útil ao gestor de TI da organização. Se a organização possui 1200 computadores com softwares antivírus e um total de 3000 computadores, por exemplo, esta métrica mostrará que apenas 40% dos computadores estão protegidos contra vírus. Esta informação é fundamental para que o gestor possa definir ações visando à melhoria da segurança. A partir desta informação, o gestor pode definir que, dentro de um mês, 100% dos computadores da empresa devem estar devidamente protegidos contra vírus. A utilização de uma métrica permite, portanto, a descoberta de um problema de segurança e o estabelecimento de uma meta, cujo cumprimento poderá ser avaliado no futuro por meio do recálculo da métrica.

Um dos principais desafios na definição de métricas de segurança é a identificação de quais métricas são eficientes e quais métricas apenas demandarão esforços e não trarão informações úteis ao gestor de TI. Além disso, métricas mal definidas ou escolhidas sem critérios podem levar a conclusões equivocadas sobre quais são os verdadeiros problemas de segurança da organização. Existem alguns parâmetros que ajudam a avaliar se uma métrica está bem definida ou não:

- A coleta dos dados utilizados para calcular a métrica não pode demandar grandes esforços da organização. É importante que o levantamento das métricas não proporcione impactos negativos ao cotidiano da organização. Os gestores devem adotar, preferencialmente, métricas cujos dados possam ser coletados automaticamente;
- As métricas devem trazer resultados quantitativos. Evite métricas cujos resultados são expressos por termos qualitativos como "alto", "médio", "baixo", "bom", "ruim", etc.;
- As métricas devem ser expressas por unidades de medida: horas, defeitos, computadores desprotegidos, etc.;
- A adoção de uma métrica deve seguir um objetivo da organização. Se o objetivo da organização é, por exemplo, diminuir a quantidade de computadores infectados por vírus e worms, as métricas devem ajudar a alcançar este objetivo. Logo, as métricas a serem adotadas neste caso devem utilizar dados como: computadores que estão protegidos por software antivírus, computadores que estão com todos os *patches* de segurança aplicados e a quantidade de treinamentos dados aos colaboradores tratando de segurança da informação.

Para facilitar a definição das métricas de segurança, podemos usar o conjunto de parâmetros listados a seguir. Para exemplificar cada um destes parâmetros, usaremos como base uma métrica que busca avaliar a porcentagem de colaboradores da organização que receberam treinamento sobre práticas seguras ao utilizar recursos de TI:

- **Identi**ficador: é um nome exclusivo dado para cada métrica a fim de organizar toda a base de métricas. Exemplo: "treinamento_seguranca_1";
- Objetivo: estabelece qual é o objetivo da implantação da métrica. Exemplo: assegurar que os colaboradores da organização estão treinados para lidar com as questões de segurança da informação;
- **Métrica**: neste atributo, deve ser inserida a definição da métrica. Exemplo: Porcentagem dos colaboradores que receberam treinamento relacionado a práticas seguras na operação de recursos de TI;
- **Fórmula**: apresenta a fórmula para o cálculo da métrica. Exemplo: número de colaboradores que receberam treinamento no último ano dividido pelo total de colaboradores da organização;

• **Alvo**: determina qual é o valor esperado para a métrica. Exemplo: dentro de dois anos, todos os colaboradores da organização devem ter recebido treinamento sobre práticas seguras no uso de recursos de TI;
• **Frequência**: estabelece a frequência na qual a métrica deve ser calculada: diariamente, mensalmente, anualmente, etc. No nosso exemplo, se considerarmos que os treinamento são dados uma vez por ano, podemos determinar a frequência de cálculo da métrica como anual;
• **Responsabilidades**: quem são as pessoas envolvidas na definição, cálculo e utilização da métrica. Em nosso exemplo, podemos colocar como responsáveis tanto o gestor de TI quanto o gestor de recursos humanos;
• **Fonte de dados**: locais onde podem ser obtidos os dados utilizados para calcular as métricas. Estas fontes podem incluir arquivos de diversos departamentos da organização, entrevistas a profissionais, inspeção de equipamentos e ambientes, utilização de ferramentas automáticas como scanners de vulnerabilidades, utilização de protocolos de gerenciamento de redes como o SNMP (Simple Network Management Protocol), etc. Em nosso exemplo, poderíamos utilizar arquivos do departamento de recursos humanos que registram os treinamentos oferecidos aos colaboradores;
• **Formato dos resultados**: determina como os resultados serão apresentados: gráfico de barra, gráfico de linhas, tabela, etc. Exemplo: a métrica sobre o treinamento dos colaboradores pode ser apresentada no formato de um gráfico "pizza";

Processo de cálculo e análise de métricas de segurança

Para que a implementação de um processo de coleta e análise de métricas de segurança funcione de maneira adequada, é importante também que a empresa possua em sua organização papéis responsáveis por responder pelas políticas e procedimentos de segurança no ambiente de TI. Um departamento ou colaborador responsável por trabalhar com a segurança da informação é essencial. A segurança da informação deve ser tratada como uma ferramenta que visa ajudar a empresa a atingir seus objetivos e não como um obstáculo para a eficiência e bom andamento da empresa. Se os procedimentos de gestão e segurança não são devidamente estabelecidos, os dados necessários para calcular as métricas não estarão disponíveis ou podem não ser confiáveis.

O processo de cálculo e análise de métricas de segurança deve ser executado de maneira contínua. Toda nova execução do processo deve ser alimentada com os resultados da execução anterior, de maneira que seja acompanhada a evolução da organização com relação à segurança da informação. A **Figura 2** apresenta as etapas do processo, que são detalhadas a seguir.

O processo se inicia com a preparação para a coleta de dados. Devem ser definidos, primeiramente, quais são os objetivos da organização com relação à aplicação das métricas de segurança. Se a organização está, por exemplo, enfrentando problemas relacionados a computadores infectados por vírus, pode estabelecer como objetivo a diminuição do número de infecções. Definido o objetivo, o próximo passo é identificar e selecionar as métricas apropriadas. A seleção das métricas deve levar em conta o custo necessário para coletar os dados e o impacto no cotidiano da organização. Métricas que podem ser coletadas automaticamente devem ter preferência. Instituições como o CIS (*Center for Internet Security*) e o NIST (*National Institute of Standards and Technology*) publicam catálogos que são bastante úteis no momento de identificar e selecionar métricas que estejam relacionadas aos objetivos da organização. Por fim, devem ser definidos os responsáveis por providenciar as ferramentas necessárias para a coleta de dados e por calcular e analisar as métricas. Toda esta etapa de preparação deve ser documentada para facilitar a execução dos próximos passos do processo.

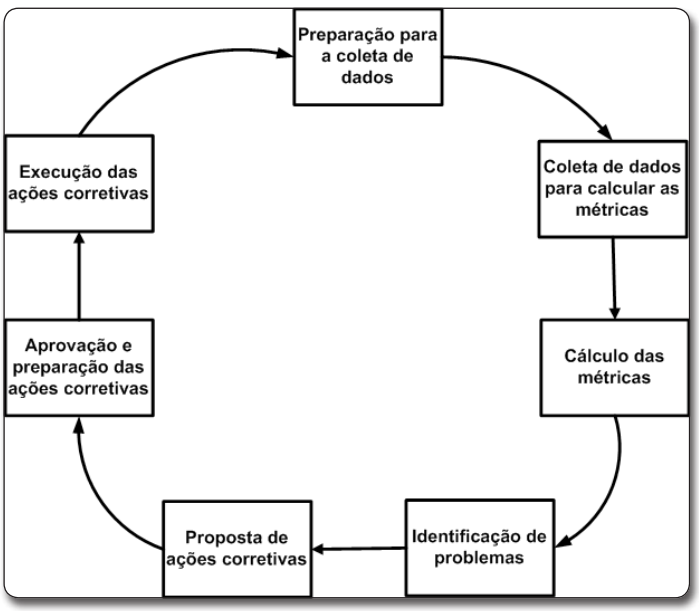


Figura 2. Processo de cálculo e análise de métricas de segurança

O próximo passo do processo é a coleta de dados necessários para calcular as métricas. Após a coleta de dados, as métricas devem ser calculadas de acordo com o previsto no atributo "fórmula" de cada métrica. De posse dos resultados calculados para cada métrica, o responsável por analisá-las deve construir gráficos e relatórios que serão estudados para que os principais problemas da organização sejam identificados.

Identificados os principais problemas, os responsáveis pela segurança da organização devem propor ações corretivas, levando em conta o custo destas ações e o impacto que elas gerarão no cotidiano da organização. Depois de definir as ações corretivas, os responsáveis pela segurança devem encaminhá-las para os departamentos responsáveis por aprovar as solicitações e, posteriormente, adquirir os recursos necessários à aplicação das ações.

O último passo do processo é a aplicação das ações corretivas para as quais houve a aprovação por parte dos responsáveis pelos recursos necessários. Após aplicar as ações corretivas, o processo volta ao seu início. Ele deve ser repetido frequentemente de forma

a acompanhar a evolução do nível de segurança da organização. Em cada rodada de execução do processo, novos objetivos podem ser incluídos ou, conforme necessidade da organização, podem ser removidos objetivos antigos.

A fim de ilustrar o processo e facilitar a sua compreensão, será apresentado um exemplo. Consideremos que a organização está buscando diminuir a quantidade de infecções por vírus. Os responsáveis pela segurança selecionaram, com base neste objetivo, quatro métricas: quantidade de infecções dividida pelo total de computadores, porcentagem de máquinas com softwares antivírus instalados e atualizados, porcentagem de máquinas com todos os *patches* de segurança aplicados e porcentagem de colaboradores que foram treinados quanto aos cuidados ao usar o computador. Depois de inspecionar os computadores da organização e consultar os arquivos do departamento pessoal, as métricas foram calculadas e os resultados mostraram que a grande maioria dos computadores possuem softwares antivírus instalados e atualizados e com todos os *patches* de segurança aplicados. Entretanto, metade dos colaboradores não participou, nos últimos três anos, de treinamentos sobre práticas de segurança. De posse destas informações, os gestores definem então que devem ser dados treinamentos aos colaboradores e devem ser reforçados os comunicados internos sobre os riscos de segurança inerentes à utilização dos computadores e da Internet. Após aprovação do departamento pessoal e do departamento financeiro, os treinamentos são realizados e o processo volta para o seu início. Os gestores devem, no futuro, coletar e avaliar estas métricas para observar se houve evolução no tratamento deste problema. É importante observar também que novas métricas podem ser avaliadas no futuro para este mesmo objetivo, de forma a garantir a solução do problema.

Exemplos de métricas de segurança

Há diversos exemplos de métricas que se aplicam a diferentes áreas de uma organização como gestão de incidentes, gestão de vulnerabilidades, gestão de mudanças, gestão financeira, infraestrutura de rede e serviços. Como exemplo, apresentaremos duas métricas para cada uma destas áreas. Na área de gestão de incidentes, temos os seguintes exemplos de métricas:

1. Tempo médio para descoberta de um incidente: esta métrica é bastante importante, pois o tempo que a organização leva para descobrir a ocorrência de um incidente está diretamente relacionado com as consequências que o incidente terá. Para calcular esta métrica, a organização precisa ter um processo de registro de incidentes, a partir do qual é alimentada uma base de dados que, entre outras coisas, armazena a data de ocorrência e a data de descoberta de cada incidente;

2. Tempo médio entre dois incidentes: esta métrica é importante, pois reflete, de maneira objetiva, o volume de incidentes que está ocorrendo na rede. É importante observar que nem sempre uma diminuição do tempo médio entre dois incidentes indica que a segurança da organização diminuiu. Mudanças que melhoram o processo de registro de incidentes podem fazer com que a organização consiga registrar um volume maior de incidentes, sem que a segurança tenha diminuído.

Na área de gestão de vulnerabilidades, temos os seguintes exemplos de métricas:

1. Porcentagem de sistemas sem vulnerabilidades graves: esta métrica pode ser calculada a partir de dados coletados por scanners de vulnerabilidade. O ideal é que a organização chegue a 100% dos sistemas sem apresentar vulnerabilidades graves. Como os *crackers* descobrem vulnerabilidades constantemente, é importante que esta métrica seja calculada frequentemente, de forma que os gestores possam acompanhar as condições de segurança neste quesito;

2. Tempo médio para solucionar uma vulnerabilidade: esta métrica reflete a eficiência da equipe de segurança em remover as vulnerabilidades descobertas após uma verificação com o scanner de vulnerabilidade. Normalmente, as soluções de vulnerabilidades são baseadas na aplicação de *patches* de correção disponibilizados pelos fabricantes do sistema.

Na área de gestão de mudanças, temos as seguintes métricas como exemplos:

1. Tempo médio para realizar uma mudança de configuração: esta métrica reflete a agilidade da equipe em realizar mudanças de configuração no ambiente de TI. Para que esta métrica seja calculada, é necessário que o setor de TI da organização tenha um processo de gestão de mudanças que registre a solicitação e o atendimento de cada uma delas;

2. Porcentagem de mudanças de configuração que receberam uma revisão de segurança: esta métrica é importante, pois indica qual é o controle de segurança sobre as mudanças realizadas no ambiente de TI. A ativação da auto configuração IPv6 em um setor da rede, por exemplo, pode criar vulnerabilidades se não forem observadas as precauções de segurança relacionadas a esta funcionalidade. O ideal é que esta métrica mostre que 100% das mudanças de configuração são inspecionadas com relação à segurança;

Na área de gestão financeira, temos os seguintes exemplos de métricas:

1. Porcentagem do orçamento da área de TI gasto com segurança da informação: esta métrica mostrará o quanto do investimento realizado em Tecnologia da Informação é empregado em segurança da informação. Não há uma porcentagem ideal para ser atingida. Os gestores devem procurar pesquisar o quanto as outras organizações no mesmo ramo de atuação têm gasto com segurança da informação para balizar os seus investimentos. Esta métrica não precisa ser calculada com grande frequência. Dependendo de como é trabalhado o orçamento da organização, esta métrica pode ser calculada uma ou duas vezes por ano. Informações importantes podem ser obtidas pelos gestores na comparação entre os resultados desta métrica ao longo dos anos;

2. Porcentagem do orçamento de segurança da informação empregado em cada área: com esta métrica, o gestor acompanha como o orçamento dedicado à segurança da informação está dividido entre áreas como gestão de incidentes, gestão de vulnerabilidades, gestão de mudanças, etc. Os gestores podem passar a fazer uma correlação entre o perfil do investimento realizado e a melhora ou piora das métricas inerentes a cada uma destas áreas.

Na área de infraestrutura, temos os seguintes exemplos de métricas:

1. Porcentagem de pontos de acesso IEEE 802.11 que utilizam o protocolo WPA2: as redes sem fio normalmente despertam uma grande preocupação com relação à segurança, já que a propagação do sinal pelo ar torna as redes sem fio propensas à interceptação de dados. Para garantir segurança nas redes sem fio IEEE 802.11, é recomendada a utilização do protocolo de segurança WPA2 (*Wi-Fi Protected Access*). Portanto, o resultado ideal para esta métrica é de 100% dos pontos de acesso IEEE 802.11 cobertos pelo protocolo WPA2. Caso o resultado não seja igual a 100%, os gestores da rede devem providenciar imediatamente a configuração dos pontos de acesso para que o WPA2 seja utilizado;

2. Porcentagem de prédios espalhados geograficamente que estão interconectados utilizando tecnologias com suporte à segurança: é comum que as organizações interliguem suas redes locais que estão espalhadas geograficamente por meio da Internet. Neste caso, para garantir que seu tráfego não seja interceptado por agentes maliciosos na Internet, a organização deve proteger estas conexões construindo Virtual Private Networks (VPNs). Esta métrica mostra qual é a proporção de conexões entre prédios da organização que está devidamente protegida. O valor ideal para esta métrica é 100%. Neste caso, a frequência de cálculo da métrica pode ser semestral, já que novas conexões entre prédios distantes não são estabelecidas com frequência.

Na área de serviços, temos os seguintes exemplos de métricas:

1. Porcentagem do tempo em que o servidor está disponível: um dos atributos mais importantes para servidores é a disponibilidade. Utilizando dados coletados por protocolos de gerência como o SNMP (*Simple Network Management Protocol*), é possível monitorar por quanto tempo os servidores operam sem interrupções. O objetivo dos gestores deve ser trabalhar para que esta métrica retorne resultados próximos de 100%. Esta métrica deve ser acompanhada em uma frequência um pouco maior. Caso os resultados estejam ruins, após a execução das ações corretivas, o acompanhamento pode ser semanal. Assim que os resultados apresentarem melhoras significativas, a frequência do acompanhamento pode diminuir passando para quinzenal ou mensal;

2. Porcentagem de chamadas VoIP completadas: nem sempre as métricas de segurança precisam trazer informações diretamente relacionadas a ataques. Informações sobre a qualidade e a confiabilidade dos serviços também são importantes para os gestores de segurança da organização. No caso desta métrica, os gestores terão informações importantes sobre o comportamento da rede VoIP da organização. O número total de tentativas de chamada e o número de chamadas completadas com sucesso pode ser verificado em IPDRs (*IP Detail Records*), que são bilhetes gerados a cada tentativa de chamada e que ficam armazenados no PABX VoIP. A frequência de cálculo desta métrica deve ser maior (semanal, por exemplo) em períodos de maiores problemas com a rede VoIP. Após tomar as medidas corretivas e obter melhoras na rede VoIP, o acompanhamento pode passar a ser menos frequente, sendo realizado mensalmente.

Conclusão

O aumento do número de incidentes de segurança tem trazido preocupação às corporações e governos em todo o mundo. A interrupção de serviços importantes e o roubo de dados sigilosos causam grandes prejuízos à imagem e às finanças das organizações. Para solucionar estes problemas, os pesquisadores e a indústria disponibilizam uma série de produtos como firewalls, sistemas de detecção de intrusão, algoritmos de criptografia, protocolos de segurança, etc. Mesmo utilizando todo este ferramental, os gestores de TI precisam saber se estão realmente seguros e se os investimentos realizados estão tendo o retorno esperado. As respostas para estas dúvidas podem ser dadas por métricas de segurança.

O cálculo e a análise das métricas de segurança formam um processo contínuo que deve ser realizado periodicamente. A realização constante deste processo permite que as lições aprendidas sejam aplicadas na melhoria do nível de segurança da organização e que o planejamento para atender futuros requisitos de segurança seja feito de forma mais fácil. Uma empresa que já conhece bem seu nível de segurança e tem realizado a coleta de métricas com frequência, provavelmente terá mais facilidade a se adaptar às novas exigências de segurança trazidas por novidades na área de TI, como, por exemplo, a migração para IPv6 ou a adoção de Computação em Nuvem.



Bruno Bogaz Zarpelão
brunozarpelao@gmail.com
Bacharel em Ciência da Computação pela Universidade Estadual de Londrina (UEL) e doutor em Engenharia Elétrica pela Universidade Estadual de Campinas (UNICAMP). Atualmente é professor da Universidade Estadual de Londrina e da PUC-PR (campus Londrina). Possui experiência de sete anos em pesquisa e desenvolvimento de soluções para gerência de redes de computadores, segurança da informação, governo eletrônico e cidades inteligentes.

Dissertação de mestrado "Aplicação de Métricas a Análise de Segurança em Redes Metropolitanas de Acesso Aberto", escrita por Rodrigo Sanches Miani
http://www.bibliotecadigital.unicamp.br/document/?code=000443391

Publicação especial do NIST (National Institute for Standards and Technology) "Performance Measurement Guide for Information Security", escrita por Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown e Will Robinson
http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

Somos tão apaixonados por tecnologia que o nome da empresa

diz tudo.

Porta 80 é o melhor que a Internet pode oferecer para sua empresa.

Já completamos 8 anos e estamos a caminho dos 80, junto com nossos clientes.

Adoramos tecnologia.
Somos uma equipe composta de gente que entende e gosta do que faz,

assim como você.





Estrutura

100% NACIONAL. Servidores de primeira linha, links de alta capacidade.



Suporte diferenciado

Treinamos nossa equipe para fazer mais e melhor. Muito além do esperado.



Serviços

Oferecemos a tecnologia mais moderna, serviços diferenciados e antenados com as suas necessidades.



1-to-1

Conhecemos nossos clientes. Atendemos cada necessidade de forma única.
Conheça!

Porta 80
WEB HOSTING

Hospedagem | Cloud Computing | Dedicados | VoIP | Ecommerce | Aplicações | Streaming | Email corporativo

porta80.com.br | comercial@porta80.com.br | twitter.com/porta80

SP 4063-8616 | RJ 4063-5092 | MG 4063-8120 | DF 4063-7486