SEGURANÇA DA INFORMAÇÃO E DE REDES

Prof. Milton Palmeira Santana

Proxy Transparente

- A premissa básica para a implantação do proxy transparente é que o usuário, ou dispositivo, não necessite executar nenhuma configuração para navegação, sendo estas atribuídas a arquitetura de segurança.

- Embora o modelo possa ser bastante atraente e de fácil implantação, existem diversos pontos que precisam ser entendidos para garantir o sucesso em sua utilização.

- O funcionamento da estrutura de proxy transparente ocorre através do redirecionamento do tráfego na porta 80 para o serviço interno do proxy, e existem muitas outras portas que podem usar o protocolo HTTP, ou o método CONNECT, que não irão passar por essa regra.

Proxy Transparente

- Muito oportuno quando você não têm acesso ao computador/dispositivo para realizar alguma configuração.

- Um aspecto interessante na implantação de proxy transparente é o recurso de caching que muitos possuem de maneira integrada. Esta facilidade permite economia de banda uma vez que os objetos da internet são armazenados em memória ou armazenamento secundário e descarregados localmente (sem o uso da internet) para usuários que requisitarem.

- Na prática, em uma rede sem proxy e caching uma requisição na internet que demanda uma atualização de 5Mb realizada por 10 equipamentos, irá gerar um consumo de internet de 50Mb, pois todos eles precisarão ir até a internet para copiar as atualizações.

Proxy Transparente

- Com o recurso de cache, o primeiro equipamento que realizar a atualização irá consultar na internet e o arquivo será armazenado no cache local. Os demais computadores ou dispositivos que requisitarem o mesmo item, vão descarregar localmente, gerando neste caso economia considerável de banda (45Mb).

- Limitações: problemas com HTTPS.

Proxy Transparente - Configuração

- Nas configurações básicas do SQUID:
  - Habilite Resolve DNS IPv4 First.
  - Habilite o modo transparente.

- Nas configurações da interface WAN:
  - Desabilitar o IPV6
  - Reserved Network: retirar para testes

- Verifique as configurações de proxy no computador cliente.

- Download do navegador Chrome.

Efetividade dos controles de segurança

- Um controle de segurança não é capaz de resolver todos os problemas de segurança isoladamente. Um firewall deixa portas abertas para serviços legítimos. Um IDS pode detectar ataques em andamento nessas portas abertas pelo firewall, porém uma ação ainda é esperada. O IPS dá uma resposta, agindo preventivamente contra os ataques em andamento, porém técnicas de evasão podem ser utilizadas. Já os antimalwares atuam no endpoint, ou no equipamento do usuário, mas mesmo assim ataques que partem de usuários contaminados causam grandes prejuízos às empresas.

- Exemplo: malware de boleto. Os números são alterados e o pagamento acaba caindo em contas de fraudadores.

Efetividade dos controles de segurança

- Além dos ataques que partem de usuários contaminados com malware, há problemas ainda mais complexos de serem resolvidos, como aqueles em que crackers roubam credenciais de usuários, passando a ter acesso a sistemas e informações críticas de uma forma direta, como se fossem os usuários legítimos. Nesse caso, os ataques não visam à exploração de vulnerabilidades de sistemas, mas sim o roubo de identidades desses usuários, normalmente com a descoberta da senha, que é o método de autenticação mais comum.

Efetividade dos controles de segurança

- Outras ameaças devem ser ainda consideradas, como o vazamento de informações confidenciais através de métodos de comunicação seguros, por exemplo, o envio de documentos de projetos para concorrentes a partir de um funcionário, por e-mail. Nesse caso, a comunicação acontece de dentro da empresa para fora, de modo legítimo e, portanto, mecanismos de segurança como firewall, IDS, IPS ou antimalware não são efetivos, já que eles visam proteger a empresa contra ataques vindos do exterior.

Efetividade dos controles de segurança

- Mesmo com todas as precauções, principalmente das agências bancárias, solicitando instalação de softwares (módulos) para segurança no navegador, por que existem ainda tantas falhas e fraudes acontecendo?

Problemas com senhas

- Um dos ataques que tem acontecido cada vez mais em todo o mundo é o que rouba credenciais dos usuários, permitindo que o cracker acesse os serviços como se fosse o usuário legítimo.

- Você já teve uma senha roubada? Repete a mesma senha em websites diferentes? Consegue memorizar senhas únicas para cada serviço que acessa?

- Senhas podem ser roubadas, descobertas ou quebradas. O roubo de senhas pode acontecer de variadas formas, por exemplo, com o envio de phishing, em um ataque no qual o usuário é enganado e passa, voluntariamente, seus dados de acesso a um serviço. Uma das técnicas de phishing é o envio de e-mail direcionando a um sítio falso, muito parecido com o verdadeiro, em que o usuário entra com suas credenciais de acesso, que são roubadas.

Problemas com senhas

- O envio do usuário a uma página falsa também pode ser feito com o ataque de DNS Poisoning ou envenenamento do DNS, em que o endereço correto é digitado em seu navegador, porém o acesso se realiza em um servidor falso.

- Outra forma de roubo de senhas é através da exploração de vulnerabilidades nos serviços (web ou banco de dados), que levam o cracker a roubar toda a base de senhas. Vários ataques desse tipo são vistos ultimamente.

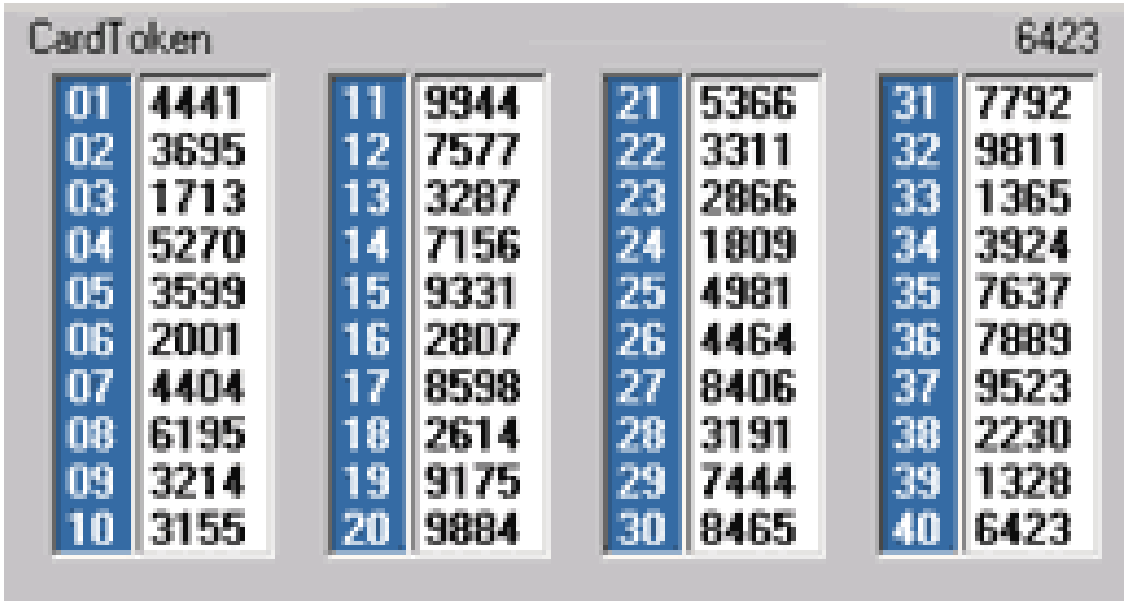
Fatores de autenticação

- A autenticação corresponde à validação de uma identidade. A pergunta que devemos fazer é: “como eu sei que o usuário é quem ele diz ser?”.

- A validação do usuário é realizada com base nos fatores de autenticação, que são três:
  - Algo que o usuário sabe: senhas ou dados pessoais (KBA, Knowledge Based Authentication).
  - Algo que o usuário possui: cartões, chaveiros ou tokens.
  - Algo que o usuário é: biometria, como impressão digital, face, voz, íris, comportamental.

Tokens

- Os tokens representam normalmente um segundo fator de autenticação, sendo utilizados em conjunto com as senhas. Há várias formas de uso do token, tais como cartões com números definidos em posições, chaveiros físicos que apresentam números ou aplicativos celulares.



Tokens

- Há ainda uma outra forma do token ser utilizado em um acesso ou transação, por meio do uso de dispositivo móvel. O provedor de serviços gera um token (código), que é enviado ao dispositivo móvel cadastrado do usuário, via mensagem de texto. Nesse caso, o segundo fator de autenticação é o próprio dispositivo móvel, em posse do usuário. Este digita o código recebido para acessar o serviço ou efetivar uma transação.

- Atualmente há variações, como o uso de código QR (Quick Response, aquelas barras bidimensionais que podem ser facilmente lidas com a câmera do dispositivo móvel), em que códigos são gerados para um acesso específico e um aplicativo é utilizado para a validação.

Tokens

- Uma característica importante dos tokens é que os números são utilizados uma única vez, sendo atualizados a cada acesso ou transação, isso faz com que os tokens sejam conhecidos também como OTP (One-Time Password), ou senha de uso único. Esse mecanismo representa o fator de autenticação baseado em algo que o usuário possui. Dessa forma, o fraudador deve roubar o cartão, chaveiro ou dispositivo do usuário para obter os números correspondentes àquele acesso ou transação.

Biometria

- A biometria representa a autenticação baseada em alguma coisa que o usuário é: pode ser baseada em alguma característica física única (impressão digital, face, voz, íris, veias) ou em alguma característica comportamental (modo de andar, modo de digitar, modo de usar o dispositivo móvel).

- Há avanços substanciais nas tecnologias biométricas e as aplicações têm aumentado a cada dia. Podemos ver a biometria sendo utilizada pelos bancos brasileiros nos caixas eletrônicos (impressão digital e veias da palma da mão) e há grande uso de biometria de impressão digital e de face em várias aplicações em dispositivos móveis.

Biometria

- Usos mais comuns da biometria:
  - **Impressão digital**: é o mais antigo e também o com menor custo para implementação. Extremamente confiável.

Biometria

- Usos mais comuns da biometria:
  - **Reconhecimento facial**: consiste em mapear o rosto. Argumentos contra: método não permanente, pois o usuário envelhece, pode realizar cirurgias, têm um irmão gêmeo.

Biometria

- Usos mais comuns da biometria:
  - **Reconhecimento de íris**: íris é a parte colorida do olho que contra a entrada de luz. É extremamente confiável, já que a membrana permanece a mesma ao longo de toda a vida. Desvantagem: Alto investimento.

Biometria

- Usos mais comuns da biometria:
  - **Reconhecimento de voz**: faz uma análise dos parâmetros físicos (cordas vocais, laringe, etc) e comportamentais, como sotaque, maneirismos, entonação, etc. Custo baixo. Confiabilidade baixa, já que qualquer ruído pode comprometer a coleta e análise da voz.

EXERCÍCIOS

1, 2 e 3 do Livro.

Introdução

- Uma das definições de criptografia diz que ela é a arte de escrever ou resolver códigos. A criptografia deriva de duas palavras gregas: kryptos, que significa oculto, e graphien, que significa escrever. O objetivo da criptografia não é esconder a existência da mensagem, mas sim de apenas ocultar o seu significado.

- De um modo geral, se a mensagem cair nas mãos de um intruso, este, ao lê-la, não a compreenderá. Apenas o remetente e o destinatário, em princípio, com um acordo pré-estabelecido (as chaves), é que têm acesso ao significado da mensagem.

- O termo criptografia é usado muitas vezes como sinônimo de criptologia, abrangendo, desta forma, a criptanálise, que tem por função descobrir os segredos ou quebrar a confidencialidade entre emissor e receptor.

Introdução

- Até o século XX, a criptografia era considerada uma arte, de modo que a construção de bons códigos, ou a quebra dos códigos, era baseada em criatividade e qualidades pessoais. Isso mudou no século 20, com o aparecimento de rigorosos estudos que fizeram a criptografia virar ciência. Antes, a criptografia tinha como objetivo a comunicação secreta, e atualmente foram acrescentados objetivos de autenticação de mensagens, assinatura digital, protocolos para troca de chaves secretas, protocolos de autenticação, leilões e eleições eletrônicas, dinheiro digital.

- Uma definição mais moderna é que a criptografia é o estudo científico de técnicas para a segurança de informações, transações e computação distribuída.

Introdução

- O público da criptografia também mudou, passando de militares e organizações de inteligência para todos, desde o acesso a websites até a proteção de informações em notebooks.

- Outra definição é que a criptografia é a ciência da cifragem das mensagens, ou seja, esconder dados e informações. É muito utilizada quando se precisam proteger informações.

- O tráfego de rede, senhas, informações em um banco de dados, normalmente são criptografadas para impedir que terceiros tenham acesso a informação.

Introdução

- Vários métodos foram inventados, desde os mais simples como a Cifra de César até os mais complexos como a criptografia quântica.

- A criptografia pode **prevenir fraudes** em comércio eletrônico e **garantir a validade** de transações financeiras.

- Usada apropriadamente, protege a anonimidade e fornece provas de identidade de pessoas.

Introdução

- A criptografia existente hoje no mercado, em alguns casos, não fornece a segurança que aprega o seu marketing.

- Bilhões de dólares são gastos em segurança de computadores, e muito é desperdiçado em produtos inseguros.

Introdução

EXERCÍCIOS – ENTREGA HOJE ATÉ AS 22:00

https://forms.office.com/Pages/ResponsePage.aspx?id=dnsOpaWOLEm_F5fWUvw86QKjc3oiHUROrSMDGNtW3MVUMEhTVVRQVVpVNFI3REdTM0VYRENPQzM3Uy4u

REFERÊNCIAS

MACHADO, Felipe Nery Rodrigues. **Segurança da Informação: princípios e controle de ameaças**. [S. l.]: ÉRICA, 2014.

FONTES, Edison. **Segurança da Informação**: O usuário faz a diferença. [S. l.]: SARAIVA, 2007.

SMULDERS, André; BAARS, Hans; HINTZBERGEN, Jule; HINTZBERGEN, Kees. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. [S. l.]: BRASPORT, 2018.

BASTA, Alfred; BASTA, Nadine; BROWN, Mary. **Segurança de computadores e teste de invasão**. [S. l.]: Cengage Learning, 2014.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. [S. l.]: Bookman Editora, 2013.

STALLINGS, WILLIAM. **Criptografia e Segurança de Redes**: Princípios e práticas. 6. ed. [S. l.]: Pearson Universidades, 2014.

SINGH, Simon. **O livro dos códigos**: A ciência do sigilo – do antigo Egito à criptografia quântica. [S. l.]: Record, 2001.


Anhanguera