Elaboração de um caderno de experimentos práticos para uso no laboratório de segurança de redes do Inatel.

Maria Tereza Yassin, Alessandra C. Domiciano, Guilherme P. Aquino, Francisco A.S. do Carmo
Instituto Nacional de Telecomunicações - Inatel
mariatereza@gec.inatel.br, alessandracarolina@get.inatel.br, guilhermeaquino@inatel.br, francisco.assis@inatel.br

***Resumo*—Atualmente no Inatel (Instituto Nacional de Telecomunicações), no curso de graduação em engenharia de telecomunicações, não há experimentos em laboratórios que ensinem características básicas sobre os principais aspectos de defesa de sistemas informatizados e conectados à Internet. Além disso, o novo currículo em vigência no Inatel prevê a existência de uma nova matéria exclusiva para exploração do conteúdo de segurança de redes e, portanto, será necessária a implantação de um laboratório para abordar esse tema dentro das dependências do Instituto.**

Para suprir essa carência, o objetivo deste trabalho de iniciação científica é gerar um caderno de experimentos práticos que pode ser usado nos laboratórios das matérias que abordem aspectos de segurança de redes. Esses experimentos levarão em consideração a utilização das defesas mais difundidas para os sistemas instalados dentro das dependências dos laboratórios e as principais ferramentas de teste de penetração deverão ser usadas para testar a qualidade dos sistemas de defesa. De posse desse caderno, professores e alunos poderão realizar experimentos de instalação, avaliação e teste de penetração para fins didáticos, aumentando o conhecimento de todos envolvidos no processo de educação dos cursos de graduação de engenharia de telecomunicações.

Pretende-se utilizar distribuições *opensources* das principais ferramentas de pentest já disponíveis e difundidas na Internet. Dessa forma, o custo de implantação destes equipamentos dentro dos laboratórios é minimizado.

***Index Terms*—Confidencialidade, Autenticidade, Integridade, Irretratabilidade, Segurança de redes, PenTest.**

I. Introdução

Quando precisamos estabelecer uma troca de dados segura por uma rede de telecomunicações, é imprescindível assegurar cinco pilares dentro dessa comunicação: i) confidencialidade, ii) integridade, iii) autenticidade, iv) irretratabilidade e, por fim, v) disponibilidade [1]. De maneira resumida, confidencialidade é tornar a informação disponível somente a quem está devidamente autorizado a acessá-la. Já integridade diz respeito a garantir que uma mensagem não sofra alterações não autorizadas. A autenticidade está ligada ao fato de um usuário ou servidor conseguir confirmar a identidade de seu correspondente. A irretratabilidade impede que o emissor ou o receptor negue uma ação realizada. E, por fim, a disponibilidade diz respeito à informação estar sempre disponível para o usuário no momento que ele precisar dela.

No ensino de segurança de redes, esses conceitos da comunicação segura podem ser melhor compreendidos se o aluno for inserido em um laboratório de experimentos práticos, onde possa vivenciar de perto como é possível habilitar esses pilares ou, até mesmo, como fraudá-los dentro de uma comunicação.

Com base nessa visão, o objetivo desse trabalho de iniciação científica é criar um caderno de experimentos práticos que aborde os pilares de confidencialidade, autenticidade, integridade e irretratabilidade. A partir dos experimentos mostrados no caderno, o aluno poderá compreender o que são e quais as implicações de se ter ou não garantidos esses pilares dentro de uma rede. Além disso, ele poderá ter acesso a uma série de ferramentas que irão ajudá-lo a estabelecer os pilares e, também, a fraudar uma comunicação segura. É claro que o intuito de fraudar uma comunicação é entender melhor as vulnerabilidades de alguns sistemas para que seja possível melhorar a defesa deles.

É importante mencionar que o caderno de experimentos foi concluído durante o período da iniciação científica e que ele se encontra disponível para uso de qualquer professor ou aluno do Inatel. Esse artigo irá fazer um resumo sobre os principais pontos dos experimentos contidos no caderno.

O texto se encontra dividido da seguinte forma. A Seção II traz uma análise dos pontos principias do experimento sobre confidencialidade e a Seção III aborda os pontos principais sobre autenticidade. As Seções IV e V trazem, respectivamente, os pontos mais importantes sobre os experimentos de integridade e irretratabilidade. Por fim, a Seção VI traz as principais conclusões desse trabalho.

II. Confidencialidade

De maneira formal, confidencialidade consiste em garantir que apenas pessoas autorizadas possam ter acesso a determinada informação. A forma mais utilizada para se instaurar a confidencialidade é a criptografia [1].

A criptografia é uma técnica que utiliza algoritmos matemáticos e senhas para cifrar e decifrar uma mensagem, visando torná-la ininteligível para terceiros e visível somente ao destinatário. Os dois tipos básicos de criptografia são a simétrica e a assimétrica [1].

A criptografia simétrica, também conhecida como criptografia de chave secreta, utiliza um algoritmo conhecido e uma única chave secreta (senha) tanto na transmissão quanto na recepção dos dados. Essa chave é utilizada tanto para criptografar quanto para decriptografar a informação compartilhada. Já a criptografia assimétrica utiliza, além de um

algoritmo conhecido, pares de chaves pública e privada que se relacionam matematicamente. Nesse processo, a mensagem é criptografada usando a chave pública do destinatário e ela só pode ser decriptografada usando a outra chave dele, a chave privada.

No caderno de experimentos existe um experimento prático de ataque à confidencialidade que implementa o cenário da Figura 1.

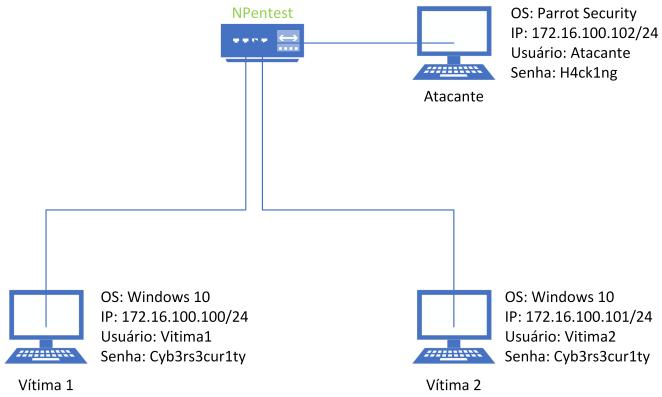

Figura 1. Cenário do experimento de ataque à confidencialidade.

Como ilustrado na Figura 1, existem três máquinas que pertencem à uma mesma rede local e são interconectadas por um switch. Vítima 1 e Vítima 2 são os dois usuários que irão compartilhar um arquivo e Atacante é o usuário que busca espionar essa comunicação e obter acesso ao conteúdo desse arquivo.

O experimento é realizado em duas partes. A primeira consiste em as duas vítimas compartilharem o arquivo confidencial em texto claro e Atacante obter acesso ao arquivo e conseguir ver seu conteúdo após monitorar a comunicação entre elas.

A segunda parte do experimento consiste em Vítima 1 criptografar o arquivo antes de enviá-lo para tentar impedir que Atacante veja seu conteúdo mesmo que consiga obtê-lo.

Durante o experimento, o aluno é direcionado a criar um arquivo de texto na máquina da Vítima 1, que será compartilhado com a Vítima 2. Isso é feito usando o esquema de compartilhamento de arquivos do Windows. Com uso da ferramenta Wireshark [2] o usuário Atacante poderá capturar todos os pacotes SMB2 (*Server Message Block*), usados para se fazer o compartilhamento do arquivo entre as vítimas. De posse desses pacotes, o Atacante poderá verificar o conteúdo do texto informado no arquivo compartilhado.

Assim, o Atacante não só consegue espionar a comunicação entre as vítimas, mas também tomar conhecimento do teor das mensagens trocadas entre elas, pois está em texto claro. Portanto, a confidencialidade da comunicação é quebrada. Os detalhes de como usar cada uma das ferramentas estão definidos no caderno de experimento.

Após observar que é possível interceptar e verificar o conteúdo de arquivos compartilhados, o aluno será conduzido a fazer um novo experimento. Nesse momento, o aluno deve repetir o experimento anterior, porém criptografando o conteúdo do arquivo antes de transferi-lo, para tentar impedir a quebra da confidencialidade. É proposto o uso do software GpgEX [3], através da interface Kleopatra, para fazer a criptografia simétrica. O algoritmo utilizado por padrão é o CAST5 [4].

Assim que o processo de criptografia do arquivo é feito, o aluno o compartilha novamente. E o usuário Atacante novamente captura os pacotes dessa comunicação. Porém, ao tentar abrir o arquivo interceptado, é preciso digitar uma senha para acessar seu conteúdo. Isso significa que, a princípio, está mantida a confidencialidade do conteúdo do arquivo, sendo seu acesso restrito somente a quem tem conhecimento da senha.

Com esse experimento é possível conscientizar o aluno sobre o problema da confidencialidade na troca de arquivos pela rede de computadores.

III. Autenticidade

A autenticidade consiste em verificar a identidade e a confiabilidade de sistemas, usuários(as), servidores, entidades, etc, na rede.

A forma mais conhecida de autenticação simples para usuários é o par login e senha, que serve como indicador para o servidor de que o usuário é realmente quem diz ser. No entanto, o par não oferece muita garantia, pois outra pessoa pode descobri-lo e utilizá-lo para acessar uma conta que não é sua. E também tem se tornado inconveniente, pois os usuários possuem cada vez mais contas em sites, os obrigando a memorizar muitas senhas.

Há outras formas de autenticação mais seguras, como as feitas em duas etapas. Dentre elas estão dispositivos token e códigos de autenticação enviados por e-mail, SMS, etc. Com isso, além de possuir o login e a senha, é preciso ter acesso ao dispositivo token, ao e-mail, ao celular, etc. do dono da conta.

Uma maneira ainda mais segura de garantir autenticidade é a utilização de certificados digitais, que identificam seus portadores em uma transação na internet. Eles possuem validade jurídica e há certificados tanto para empresas quanto para pessoa física. O certificado é emitido por uma Autoridade Certificadora e pode ser armazenado na máquina do utilizador ou em um dispositivo externo, como token USB ou cartão inteligente. Ele contém informações como o nome do utilizador, prazo de validade e chave privada (utilizada para assinaturas digitais).

Quando um usuário acessa um site certificado, o servidor do site envia seu próprio certificado digital para provar que ele é quem diz ser. Essa transferência é feita através do protocolo SSL (*Secure Sockets Layer*) que, além de permitir verificar a autenticidade de servidor e cliente, provê confidencialidade nos dados trocados.

No caderno de experimentos, o aluno deve montar uma rede, cujas topologia e configurações de máquinas são ilustradas na Figura 2.

O experimento é realizado em duas partes: A primeira consiste em Atacante clonar a página de login do site “testphp.vulweb.com", que é HTTP, e Vítima 1 ser direcionada para a página clonada ao fazer o acesso. Dessa forma, atacante recebe os dados fornecidos por Vítima 1 no site falso.

A segunda parte do experimento consiste em Atacante clonar a página de login do site “facebook.com.br", que é

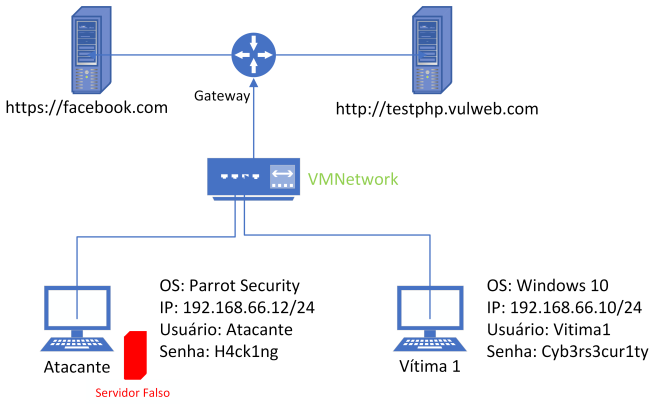

Figura 2. Cenário do experimento de ataque à autenticidade.

HTTPS, e Vítima 1 verificar sua autenticidade através do Certificado Digital, evitando ser enganada.

Para clonar os sites em questão, o aluno deve utilizar o programa `Social Engineering Toolkit`, que é uma ferramenta desenvolvida para facilitar a execução de ataques do tipo Engenharia Social. Na máquina Vítima 1, foi feita uma configuração de DNS, direcionando endereço `testphp.vulnweb.com` para o endereço IP da máquina Atacante. O mesmo foi feito com o endereço `facebook.com.br` para a segunda parte do experimento. Portanto, quando a vítima tentar acessar qualquer um dos sites citados, ela será erroneamente direcionada para a máquina do atacante que contém um clone perfeito do site desejado.

No primeiro caso, ao entrar com o Login e a Senha no site clonado a Vítima 1 fornece seus dados a um site falso. Para Vítima 1, não há como saber que o site que ela acessou primeiro não é o verdadeiro, pois o site legítimo não possui um certificado digital que possa ser verificado. No segundo caso, ao acessar o facebook, a vítima também será redirecionada, porém, o navegador não irá apresentar as informações do certificado digital. Ao analisar essa questão, o aluno poderá verificar que se trata de um clone e, portanto, não irá fornecer suas credenciais.

Como principal conclusão, o aluno pode verificar que os sites clonados pelo SEToolkit são HTTP e não apresentam o certificado digital do site original, quando estes são HTTPS. Dessa forma, é possível para o usuário saber que não está acessando o site verdadeiro quando se trata de uma cópia de site HTTPS, basta verificar a ausência do certificado digital. Os navegadores sempre alertam sobre os sites HTTP, informando que não são seguros. Esses sites, além de não serem autenticados, também não implementam nenhum tipo de criptografia que garanta a confidencialidade dos dados transmitidos na rede, devido a não utilização do protocolo SSL.

IV. Integridade

Garantir a integridade de um arquivo, mensagem ou programa é prevenir adulterações de suas informações ou funções por pessoas não-autorizadas, assim como evitar que eles sejam destruídos sem autorização. Garantir a integridade também é prevenir que erros ou modificações em sistemas corrompam dados de arquivos, mensagens ou programas.

Uma forma de se assegurar a integridade de dados transmitidos é através de funções Hash. Funções Hash são funções matemáticas que comprimem entradas de tamanhos arbitrários em saídas de tamanhos fixos. As funções de Hash mais conhecidas são: MD5(*Message Digest* 5), SHA-1(*Secure Hash* 1) e SHA-256 (*Secure Hash* 256) [1].

Quando duas ou mais entradas distintas geram o mesmo valor de hash ocorre uma colisão. A probabilidade de ocorrência de colisões de Hash é um parâmetro utilizado para aferir a segurança da função. Ou seja, quanto menor a probabilidade de colisão, maior é a segurança da função Hash.

Uma outra forma de garantir integridade é através do código de autenticação de mensagens (MAC – *Message Authentication Code*). Seu funcionamento é similar ao Hash, porém, é preciso que as partes envolvidas na troca das mensagens possuam uma chave secreta, para que o código MAC seja gerado. Suas entradas são uma mensagem de tamanho arbitrário e a chave secreta, e sua saída é um código de comprimento fixo. Ao se alterar a mensagem, é preciso possuir a chave secreta para gerar um novo MAC compatível. Caso contrário, ao se verificar a integridade da mensagem, os MACs serão diferentes, e a mensagem não será considerada íntegra.

O experimento criado para esse pilar deve ser feito utilizando a máquina Linux Atacante. O experimento é realizado em duas partes. A primeira consiste em o funcionário adulterar o arquivo que contém suas informações e, posteriormente, o responsável pelos pagamentos implementar um sistema que garanta a integridade dos dados utilizando Hash. A segunda parte do experimento consiste em utilizar a função MAC para o mesmo fim.

Primeiramente o aluno cria um arquivo que contém alguns dados verdadeiros sobre um funcionário de uma empresa, como, por exemplo, dados bancários. Depois, o Atacante cria uma cópia do arquivo e altera algum dado dele, simulando uma fraude. Após isso, é gerado o hash do arquivo original e ele é anexado ao arquivo, no intuito de possibilitar a verificação de sua integridade. No entanto, o mesmo é feito com o arquivo adulterado. Assim, o aluno irá concluir que a técnica de anexar o Hash ao arquivo nem sempre é segura. Ela somente previne fraudes se apenas o conteúdo do arquivo for alterado. No caso de um terceiro malicioso gerar um novo Hash com as informações alteradas, não será identificada a fraude.

Para se evitar uma fraude como a descrita acima, pode-se utilizar uma outra técnica com um nível maior de segurança, o MAC. Portanto, num segundo momento, o aluno repete o experimento, mas utilizando a função MAC em vez de Hash. Assim, ele pode verificar como essa função pode ser usada para prevenção de ataques à integridade das mensagens.

Todos os passos são listados no caderno de experimento, juntamente com um tutorial de uso das principais ferramentas usadas.

V. Irretratabilidade

Irretratabilidade, ou não-repúdio, é garantir que ações sejam atribuídas indubitavelmente a quem as executou. Estas ações podem ser criação, envio e exclusão de documentos e e-mails, instalação e desinstalação de programas, dentre outras.

Para garantir a irretratabilidade, faz-se o uso da assinatura digital, uma aplicação muito importante da criptografia assimétrica [1]. Como foi visto na sessão sobre confidencialidade, a criptografia assimétrica utiliza uma chave privada e uma pública, relacionadas matematicamente. Na assinatura digital, a chave privada do emissor é utilizada para assinar uma ação, documento ou mensagem, e sua chave pública é utilizada como entrada para a verificação da assinatura.

Uma forma de se facilitar a criação e a verificação de uma assinatura digital, bem como otimizar o armazenamento de assinaturas, é embutir uma função de Hash no esquema da assinatura. Nesse caso, o Hash da mensagem é criptografado utilizando-se a chave privada do emissor. Para verificar a veracidade da assinatura, o receptor gera localmente o Hash da mensagem e este é comparado com o resultado da decriptografia da assinatura do emissor. Caso os Hashs sejam iguais, a assinatura é validada. Como a chave privada usada inicialmente pertence ao emissor específico, ele não poderá negar que fez tal ação, fazendo com que a irretratabilidade esteja presente na conversação.

Os meios mais comuns de assinatura digital são através de ferramentas como Kleopatra, de Tokens USB e de Smart Cards. Os dois últimos são dispositivos físicos e as principais diferenças entre eles são que Tokens USB podem ser conectados diretamente no computador e SmartCards precisam de leitores de cartão para que funcionem.

Assinaturas digitais podem ser utilizadas para substituir assinaturas em documentos físicos, como contratos, pois possuem validade jurídica equivalente ao reconhecimento de firma em cartório. Além disso, muitas empresas bloqueiam seus sistemas e só é possível utilizá-los ao conectar um pendrive que assina as ações. Dessa forma, cada ação de um funcionário é assinada digitalmente e, portanto, o funcionário não poderá negar uma ação que ele tenha feito dentro da empresa.

No experimento proposto, o aluno assina e verifica assinaturas de documentos, assim como observa o que acontece quando o conteúdo de um arquivo assinado é modificado. O aluno é instruído a criar o par de chaves pública e privada, utilizado para a assinatura digital, a partir da aplicação Kleopatra. Depois, os alunos devem trocar e-mail com documentos assinados digitalmente e verificar as assinaturas dos documentos recebidos.

Com esse simples experimento, os alunos podem verificar como gerar e verificar as assinaturas digitais em documentos e ações. Todos os passos para tal tarefa estão listados no caderno de experimento.

VI. Conclusão

Esse artigo resume as experiências práticas que compõem o caderno de experimento que será usado na disciplina de segurança de redes do Inatel. Foram desenvolvidas experiências que guiam o aluno em seus estudos práticos sobre os principais conceitos de segurança cibernética: i) confidencialidae, ii) autenticidade, iii) integridade e iv) irretratabilidade. Com o uso do caderno de experimento o aluno terá uma maior aproximação com as ferramentas que auxiliam tanto em ataques quanto nas defesas dos sistemas de segurança aplicados às redes de telecomunicações.

Referências

[1] W. Stallings, *Criptografia e segurança de redes: princípios e práticas*. Pearson, 2014.

[2] Wireshark.org, “Go deep with wireshark.” disponível em, https://www.wireshark.org.

[3] GPGEx, “Gpg4win - a secure solution.” disponível em, https://www.gpg4win.org.

[4] T. G. C. project, “Class cast5.” disponível em, https://www.gnu.org/software/gnu-crypto/manual/api/gnu/crypto/cipher/Cast5.html.