TÉCNICAS DE INVASÃO: UM ESTUDO SOBRE AS ARMAS DO MUNDO DIGITAL[*]

Taís Cristina da Silva– UEMG/Unidade Carangola
Diêgo Pereira Lozi– UEMG/Unidade Carangola
Gabriel Aguiar Tinti de Souza– UEMG/Unidade Carangola
Lucas Borcard Cancela – UEMG/Unidade Carangola

RESUMO: Ao conectar-se à internet, é preciso que o usuário se atente ao fato de que ninguém está 100% seguro na rede. Sendo assim, certas medidas relativas à segurança são essenciais para uma navegação segura. Este artigo tem por objetivos: discorrer sobre o uso de técnicas de invasão em redes e dispositivos eletrônicos, mostrando as principais técnicas existentes, assim como as ameaças e ataques mais aplicados no cotidiano; apresentar técnicas com as quais pode-se testar um sistema ou rede com o objetivo de descobrir, mapear e expor possíveis vulnerabilidades. Portanto, o artigo expõe os problemas e direciona a soluções para estes através de medidas preventivas e corretivas. A metodologia utilizada trata-se de pesquisas qualitativas, que tiveram por base estudos bibliográficos e de páginas da web para a elaboração do presente artigo. O tema foi escolhido devido ao crescimento contínuo de pessoas conectadas na grande rede, a saber, a internet, e ao grande avanço das tecnologias, as quais são alvos constantes de ataques cibernéticos. Enfim, é importante destacar neste trabalho que conhecimento e responsabilidade devem sempre agir com indissociabilidade, visto que o conhecimento não é crime mas, ataques digitais, são. Sendo assim, é preciso que os usuários conheçam possíveis ameaças para se defender, usando o conhecimento com responsabilidade.

PALAVRAS CHAVE: Técnicas de Invasão; Vulnerabilidades; Ataques; Medidas de Prevenção.

INTRODUÇÃO

No início da utilização das redes de computadores, permitiu-se que usuários trocassem mensagens e compartilhassem arquivos e periféricos. Com o passar do tempo, a importância da conectividade assim como o aumento de usuários fizeram com que várias outras aplicações fossem criadas como sistemas bancários online, o *e-commerce* e a possibilidade de realizar tarefas sem sair de casa através da utilização das redes.

A partir disso, percebeu-se uma maior vulnerabilidade por parte dos usuários com relação ao uso das redes, e, com isso, um aumento dos problemas relacionados à segurança que podem ser causados de forma intencional por pessoas que procuram obter ilicitamente algum benefício ou simplesmente prejudicar alguém.

Entende-se que as técnicas de invasão, não servem apenas para verificar redes e sistemas com o intuito de identificar vulnerabilidades, mas que, popularmente tem sido usadas por criminosos virtuais, que utilizam a fim de obter acesso a informações confidenciais de um indivíduo ou uma organização, podendo resultar no comprometimento da integridade dos dados do seu alvo.

Nesse sentido, pode-se explorar a parte de contramedidas com a finalidade de prevenção e até proteção contra invasores maliciosos. E em caso de ataques consumados, tais medidas

[*]XIV EVIDOSOL e XI CILTEC-Online - junho/2017 - http://evidosol.textolivre.org

também são cabíveis, pois em alguns casos elas podem servir de instruções para a solução do problema e garantir a rede, dispositivo ou indivíduo afetado a restauração de seus dados.

1. CONCEITUANDO TÉCNICAS DE INVASÃO

Uma invasão em informática, é conceituada como um mecanismo utilizado para procurar por falhas ou informações refinadas em redes ou dispositivos eletrônicos. Segundo Moreno (2015, p, 51), uma técnica de invasão pode ser tida como:

> Uma bateria de testes metodológicos normalmente aplicados em redes de computadores e sistemas operacionais, podendo ser direcionados também a web sites, redes sem fio, banco de dados, aplicativos e programas, com o objetivo de descobrir, mapear e expor todas as possíveis vulnerabilidades.

Um teste de invasão, é baseado em uma tentativa de incursão por partes, onde o objetivo principal é explorar brechas e quebrar os pilares básicos da segurança da informação em situações cotidianas, para avaliar a segurança de uma rede e identificar os seus pontos mais vulneráveis.

Contudo, não existe uma invasão de fato, sem que existam responsáveis por isso. Estes podem ser conhecidos como: *hackers* e *crackers*[1] ou então como, *pentesters* ou analistas de segurança da informação. Todos eles usam os seus conhecimentos para se dedicarem a testar os limites de um sistema, avaliando a qualidade de segurança de um alvo ou para estudo e procura de conhecimento. Em outros casos, invadem por pura curiosidade, ou ainda, por simples prazer.

No entanto, Moreno (2015, p. 52) ressalta que,

> uma invasão pode ser realizado por criminosos virtuais, que terão acesso as informações confidenciais que comprometem a integridade dos dados digitais de seu alvo. De posse de tais informações confidenciais, a rede que é alvo de um ataque digital pode sofrer consequências que vão depender da vontade do criminoso virtual:
>
> - Roubo e disseminação na web de informações confidenciais e arquivos sigilosos.
> - Roubo e sequestro de senhas de acesso a servidores e máquinas vitais ao funcionamento da rede.
> - Roubo de senhas de internet banking.
> - Uso de qualquer informação confidencial para benefício próprio.
> - Instalação de vírus e programas para acesso remoto (backdoors).
> - Uso de rede e dos computadores como "laranja" para outros crimes virtuais.
> - Perda de faturamento financeiro devido a ataques de negação e paralização de serviços e internet na rede vítima.

Existem muitas ferramentas para facilitar uma invasão e a cada dia aparecem novidades a esse respeito.

[1] Em tese, hackers e crackers são pessoas que possuem extrema habilidade com computadores e redes. Segundo Aspis (2009, p.56), "o que fundamentalmente diferencia hackers de crackers é a ética na qual está baseada a atividade de cada um desses grupos". Pois, um hacker é o indivíduo que elabora e/ou modifica softwares e hardwares de computadores de forma legal, para fortalecer ou melhorar a segurança da máquina ou sistema. Já um cracker, é o indivíduo que pratica atos ilícitos, como a quebra no sistema de segurança de um software ou rede para roubar e disseminar dados sigilosos.

1.2 Principais Técnicas de Invasão

Assim como existem diferentes tecnologias a serem exploradas, há também diferentes tipos de ataques, que podem ser categorizados em ativos e passivos. Estes são utilizados tanto em infraestruturas de segurança de redes como em estações de trabalho.

Ataques ativos geralmente alteram o sistema ou rede atacada, afetando a disponibilidade, integridade e autenticidade dos dados; já os ataques passivos, visam obter informações, comprometendo a confidencialidade dos dados.

1.2.1 Reconhecimento e Coleta de Dados

Essa técnica consiste no momento em que o invasor realiza a coleta dos dados de seu alvo e o reconhece, ou seja, realiza um "reconhecimento de terreno" para então atacar. Esse reconhecimento pode ocorrer de três formas, reconhecimento ativo, reconhecimento passivo e o chamado *sniffing*.

O primeiro, consiste em um reconhecimento e coleta de informações da vítima sem que a mesma esteja ciente, logo é uma invasão propriamente dita; o segundo, consiste em um rastreamento de mídias sociais e outros meios onde a vítima expõe suas informações para coletar as mesmas; e o terceiro, corresponde a um monitoramento do trafego de dados da vítima, onde são coletados vários endereços de IP, servidores e redes ocultas que a vítima possui.

Rocha (2015, p. 143), faz uma definição curta e clara ao citar que, reconhecimento e coleta de dados "compreende as atividades de reconhecimento ativo e passivo, com a finalidade de coletar informações sobre o alvo, e estabelecer uma imagem do alvo ou footprint que permita ao Hacker avaliar e escolher a melhor forma de ataque".

1.2.2 Varredura de Rede

A varredura de rede, também conhecida como *scan*, é uma busca realizada em uma rede, com o objetivo de encontrar computadores ativos dentro dela, e, com isso, coletar o máximo de informações possíveis. Com as informações coletadas na varredura, o usuário que realizar o ataque pode encontrar vulnerabilidades relacionadas a programas instalados na máquina e também serviços ativos na mesma.

As varreduras de rede podem ser realizadas de duas formas, onde ambas exploram as vulnerabilidades da máquina. Essas formas são a legítima e a maliciosa.

A forma legítima é realizada por pessoas autorizadas, ou seja, profissionais da área. O profissional realiza varreduras em computadores para verificar a segurança da rede e assim, tomar as devidas medidas para prevenir ataques.

A forma maliciosa já é realizada por pessoas que tem más intenções. Ou seja, realizam ataques em busca de vulnerabilidades para roubar informações e realizar atividades maliciosas.

1.2.3 Códigos Maliciosos

Os códigos maliciosos, conhecidos no ramo de TI como *malwares*, são programas desenvolvidos com o intuito de realizar atividades maliciosas.

Quando um *malware* é instalado na máquina da vítima, a pessoa que realiza o ataque consegue acesso com permissões de administrador, podendo realizar ações como se fosse o usuário, além de ter acesso a todas as informações contidas no computador.

Há vários motivos que levam uma pessoa desenvolver um código malicioso. Muitas das vezes o desenvolvedor do código tem a intenção de obter vantagens como roubo de informações confidenciais, práticas de golpes, ataques e também distribuição de *spam*.

1.2.3.1 Vírus

O Vírus é considerado um programa malicioso, ou parte dele, que é instalado na máquina através de um e-mail malicioso, sites da internet, pen-drives, entre outros. Ele se

espalha facilmente, tornando outros programas e arquivos infectados através de cópias de si mesmo. Mas, vale lembrar que para a sua disseminação na rede ou dispositivo, o arquivo que hospeda o vírus precisa ser executado.

Existem diversos tipos de vírus, os mais comuns são o vírus por e-mail, vírus de script, vírus de macro e vírus de celular.

O vírus por e-mail é feito através de um e-mail enviado com um arquivo em anexo. Este arquivo malicioso infecta os arquivos do computador do usuário, além de se redirecionar para os e-mails salvos na lista de contatos do usuário. Para ser executado, o usuário precisa abrir o arquivo anexo no e-mail.

O vírus de script, é um vírus que quando implantado no computador da vítima através do acesso uma página da web ou de um e-mail ou por arquivos em anexo, é chamado de vírus de script, pois é escrito em linguagem de script, como Java Script ou VBScript.

O vírus de macro é escrito na linguagem macro e infecta softwares que utilizam esta linguagem. Um exemplo de software que utiliza a linguagem macro são os programas do pacote Microsoft Office, como o Word, Excel, Power Point e outros.

O vírus de celular é disseminado por meio da tecnologia Bluetooth e por meio de mensagens de texto MMS (Multimedia Message Service). A infecção acontece da mesma forma que as outras, quando o usuário recebe e executa o arquivo infectado. No caso do celular o vírus pode remover ou modificar arquivos, contatos, realizar ligações e tentar se transmitir para outros aparelhos.

1.2.3.2 Spyware

O *spyware*, é um software que tem como objetivo, monitorar as atividades da máquina do usuário e repassar as informações coletadas, trabalhando como um espião. Ele pode ser usado de forma legítima ou maliciosa, levando em consideração aspectos como as ações feitas, o modo como é instalado, informações monitoradas, o uso e quem recebe as informações.

A forma legítima, é quando o próprio usuário instala em sua máquina ou com a liberação do mesmo para que seja verificado se há pessoas utilizando a máquina de modo abusivo ou sem autorização.

Já o malicioso, é quando são realizadas ações sem autorização, que podem prejudicar a privacidade do usuário. Geralmente utilizados para capturar informações do usuário como histórico de navegação ou informações registradas em softwares, como usuário e senhas.

1.2.4 Negação de Serviços (DoS e DDoS)

O DoS é um ataque, que tem por objetivo impedir que uma máquina tenha acesso a determinado serviço. Se utilizado de forma coordenada e distribuída, ou seja, inserido em um grupo de computadores, passa a ser uma negação de serviço distribuído ou DDoS.

O método utilizado nesses ataques costuma ser o de congestionar o servidor fazendo com que o mesmo não possa dar resposta, ou seja, enviando um número de solicitações ao servidor que seja superior ao número que ele suporta, impedindo que o mesmo envie o serviço requerido.

A finalidade desse serviço não é invadir ou roubar informações do alvo, mas sim causar indisponibilidade de serviços. Após o ataque ser realizado com sucesso, todos os usuários dependentes dos recursos afetados perdem acesso tornando impossível realizar operações.

Existem diversas formas de realizar ataques DoS ou DDoS. Os mais conhecidos são, pela grande quantidade de solicitações feitas a um determinado serviço, consumindo recursos e impedindo que as solicitações sejam completadas. Ou, ocupando toda a banda disponível através de geração de tráfego, deixando indisponível qualquer acesso ou serviço de uma rede.

2. ANÁLISE DAS VULNERABILIDADES

A pesquisa por Vulnerabilidades é o procedimento para a descoberta de pontos fracos de um projeto, que poderia favorecer um ataque ao sistema.

Moreno (2015, p.55) considera que, "na análise de vulnerabilidades, é feito apenas um levantamento de falhas encontradas sem usar o verdadeiro 'poder de fogo' de um teste de intrusão, não relatando se realmente a vulnerabilidade existe ou não". E que, portanto, seria necessário um mapeamento de vulnerabilidades para melhor detecção de falhas.

Nesse sentido, o autor explica que:

> O mapeamento de vulnerabilidades consiste na identificação e análise das possíveis vulnerabilidades. Uma vez que as etapas de coleta de informação, descobrimento, enumeração dos alvos, serviços e portas foram efetuadas, está na hora de investigar as possíveis vulnerabilidades que existem no alvo que poderão comprometer toda a rede em questão (MORENO, 2015, p. 132).

3. CONTRAMEDIDAS E SOLUÇÃO PARA ATAQUES

Dentre as inúmeras técnicas de invasão existentes, existem métodos que podem ser utilizados como medidas preventivas e/ou medidas para auxiliar em caso de ataques. Elas aumentam relativamente a segurança do usuário, e caso não sejam aniquiladas as chances de haverem estes ataques, servem para diminuir consideravelmente as chances de que ocorreram ataques.

As contramedidas e medidas de defesa podem ser referidas na maioria das vezes para cada tipo específico de ataque. O Acúmulo de informações, Coleta de dados, Varredura de rede e Códigos maliciosos são tipos de ataques que realizam um apanhado de informações da vítima a partir de uma série de varreduras; as contramedidas para conter este ataque segundo Microsoft Corporation (2004) são:

> Efetuação de configuração dos roteadores de modo que restrinja reações do mesmo a requisições de footprinting e Configuração dos sistemas operacionais que realizam a hospedagem de softwares de rede evitando o footprinting para deixar inabilitados os protocolos que não são usados e as portas que não são necessárias.

3.1 IDS – Sistema de Detecção de Intruso

O IDS, ou sistema de detecção de intrusão corresponde as formas técnicas de se realizar a identificação de uma invasão na rede, seja por pessoas externas à determinada organização ou até mesmo funcionários que não tenham autorização para manusear e acessar tal rede. Vale ressaltar que com os avanços tecnológicos na área, a identificação deste tipo de invasões está se tornando cada vez mais complexa e difícil.

Silva e Julio (2014) definem que:

> O Sistema de Detecção de Intrusão (IDS) pode ser utilizado em ambientes corporativos, assim como em redes locais, dependendo de seu modelo empregado. Basicamente tem-se um modelo baseado em host e outro baseado em rede. Sua funcionalidade principal é servir como uma segunda linha de defesa à invasão, agindo posteriormente à constatação da intrusão no sistema. Sistemas neste caso pode ser a rede, um servidor ou um computador pessoal analisando as atividades da rede ou do computador em questão.

Dentre os trabalhos realizados pelo IDS para dificultar as ações dos invasores, vale destacar aqueles que são realizados utilizando SSL e também o IPSec. O primeiro faz o papel de autenticar os pacotes de determinado terminal, essa ação dificulta extremamente a atividade

dos invasores, levando em conta que com a criptografia, um pacote sai criptografado de um terminal e só é descriptografado no destino final, impedindo ações de intermediários. Já o segundo, funciona de modo semelhante ao primeiro, mas com a diferença de que ele enfatiza a forma com que essas informações são criptografadas, podendo autenticar fragmentos do pacote em camadas pelo SSL, ou em túnel, onde o pacote inteiro é criptografado para o envio.

4. CONCLUSÃO

O presente artigo trouxe inúmeras informações a respeito das técnicas para realizar invasões, abordando conceitos e explicações, listando as principais técnicas, entre outros. Entende-se portanto, que as técnicas de invasão não servem apenas para verificar redes e sistemas com o intuito de identificar vulnerabilidades, mas também, com a intenção de invadir redes e dispositivos para obtenção de acesso a informações confidenciais de um indivíduo ou uma organização, podendo resultar no comprometimento a integridade dos dados do seu alvo.

A partir disso, percebeu-se que nada nem ninguém está seguro diante de tanta tecnologia exposta. Principalmente pelas vulnerabilidades por parte dos usuários, com relação ao uso desses atrativos. E, com isso, um aumento dos problemas relacionados à segurança que podem ser causados de forma intencional por pessoas que procuram obter ilicitamente algum benefício ou simplesmente prejudicar alguém.

Por isso, é importante lembrar àqueles que projetam, criam ou utilizam de dispositivos tecnológicos, que além de medidas de prevenção ou contramedidas em caso de ataques maliciosos, estes indivíduos podem ser amparados pelo Código Penal Brasileiro, que no artigo 154-A afirma como sendo crime, qualquer tipo de invasão a dispositivos alheios conectados à rede ou não, violando o mecanismo de segurança sem a autorização do titular. Portanto, qualquer indivíduo praticante de tal ato, a fim de colocar em risco a segurança de pessoas comuns, empresas ou grandes organizações, estará sujeito a pena de três meses a um ano de reclusão e pagamento de multa.

REFERÊNCIAS

ASPIS, Renata Lima. Hackerismo como resistência política. In: AMARAL, Sérgio Ferreira do; PRETTO, Nelson De Luca (Organizadores). *Ética, hacker e a educação.* Campinas, SP: FE/UNICAMP, 2009. Cap. 5, p. 53-67.

BRASIL. *Código Penal Brasileiro. Decreto-Lei nº 2.848, de 7 de Dezembro de 1940.* Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 18 mai. 2017.

CORPORATION, Microsoft. *Ameaças e contramedidas de segurança na web.* TechNet. 2004. Disponível em: <https://technet.microsoft.com/pt-br/library/dd569900.aspx >. Acesso em: 17 nov. 2016.

MORENO, Daniel. *Introdução ao Pentest.* Novatec. São Paulo, SP, 2015.

ROCHA, Waurlênio Alves. *Hacker Ético, conceitos e técnicas.* Eripi. 2015.

SILVA, Edelberto Franco; JULIO, Eduardo Pagani. *Sistema de Detecção de Intrusão - Artigo Revista Infra Magazine 1*. DevMedia. 2014. Disponível em: <http://www.devmedia.com.br/sistema-de-deteccao-de-intrusao-artigo-revista-infra-magazine-1/20819 >. Acesso em: 20 nov. 2016.