10ª Jornada Acadêmica da Jornada da UEG
"Integrando saberes e construindo conhecimento"
10 a 12 de Novembro de 2016
UEG - Câmpus Santa Helena de Goiás, GO

COMO INVADIR SISTEMAS COMPUTACIONAIS?

Danilo Nunes de Assis[1]; Gerson Everton de Borba Lopes[1]; Glauco Vitor Pedrosa[2]; Thamyris Furquim Martins[1]; Victor Lucas Soares Freitas[1]; Wellington Barbosa de Jesus[1];

[1]Discente do curso de Sistemas de Informação da UEG-Câmpus Santa Helena de Goiás, dnanunes@outlook.com; everton.doze@hotmail.com; thamyriisf.m@hotmail.com; vlucas981@gmail.com; wellington_ueg@hotmail.com;
[2]Docente do curso de Sistemas de Informação da UEG- Câmpus Santa Helena, glaucovitor@gmail.com;

Resumo

Com a chegada da internet as redes de computadores não param de crescer, o que faz com que apareçam novas tecnologias, e conseqüentemente, novas vulnerabilidades. Qualquer dispositivo que tenha acesso à internet está sujeito a sofrer diversos tipos de ataques, muitas vezes causando prejuízos e danos enormes às vítimas. Alguns desses ataques podem ser devastadores nas organizações. Assuntos relacionados a métodos de Invasão, Testes de Intrusão ou Testes de Penetração (*Pentest*), são termos que dizem a mesma coisa e são utilizados pelos administradores de rede para buscar e realizar tratamento das vulnerabilidades encontradas na empresa, simulando ataques como se fossem reais nas redes e sistemas de informação. Devido a este contexto, é importante que se façam testes de intrusão para ver a real segurança dos ativos (qualquer bem que tenha valor para a organização) de rede para que não sejam comprometidas a integridade, disponibilidade e confidencialidade das informações. O objetivo deste artigo é mostrar alguns dos muitos métodos utilizados por hackers para invadir um sistema computacional, verificando as falhas de segurança encontradas antes que outros o façam, buscando prevenir assim contra os ataques reais. Ao longo do artigo serão demonstradas algumas técnicas e ferramentas para realização *de invasão de sistemas computacionais*, identificando vulnerabilidades no ambiente corporativo.

Palavras-chave: Tecnologia da Informação; Segurança da Informação; Software Malicioso; Ataque Hacker; Redes;

1. INTRODUÇÃO

A Internet surgiu em 1969, nos laboratórios de pesquisa dos Estados Unidos *ARPAnet* (*ARPA - Advanced Research Projects Agency*), a qual era uma rede interna do Departamento de Defesa Norte-Americano e se tornou pública a partir da década de 1990, e tem crescido bastante nos últimos anos. A cada dia, a sociedade está mais dependente das tecnologias, as pessoas não conseguem mais viver sem água, luz e agora sem internet. O sucesso da Internet mudou consideravelmente as rotinas do mundo todo, trazendo prós e contras desse mundo virtual como também é chamado o espaço cibernético ou *cyberspace*. Ele é formado por uma rede de computadores interconectada, onde tramitam informações de todo planeta. Porém, nesse espaço onde milhares de pessoas trabalham todos os dias, surgiu também a insegurança, que pode ser descrita como as vulnerabilidades, ameaças e pragas virtuais. Muitas empresas começaram a utilizar a rede mundial de computadores para realizar transações financeiras e comerciais. Com isso, a parte de negócio das organizações ficou mais suscetível às novas ameaças, além de que novas tecnologias vão surgindo a cada minuto, sendo em alguns casos embutidas de vulnerabilidades as quais, se exploradas por pessoas indevidas, podem causar prejuízos à empresa. Até mesmo sites do governo e grandes empresas como a Sony (2011), Aplle de acordo com o jornalista Pereira (2012), o grupo *hacker AntiSec* divulgou uma série de informações e dados de usuários da Apple têm sofrido uma série de ataques cometidos por *hackers*.

Encontrar falhas de segurança num sistema de informação não é uma tarefa fácil, mas é importante procurar se prevenir de ataques reais. É necessário que seja realizado um planejamento para monitorar toda infra-estrutura de Tecnologia da Informação (T.I.), para observar possíveis ataques através de simulações de ataque. É ideal uma abordagem de forma proativa que identifique as vulnerabilidades existentes, buscando soluções capazes de reduzir o risco da empresa.

A seguir, serão abordados alguns tipos mais comuns de ataques sofridos em sistemas computacionais, trazendo detalhes de como é realizado.

2. FUNDAMENTAÇÃO TEÓRICA

2.1.Spoofing and Port Scanners

Scanners são programas de varredura utilizados para detectar possíveis vulnerabilidades em sistemas. Em outras palavras, eles são programas procuram por certas falhas de segurança que podem permitir ataques e até mesmo invasões. Mesmo que se tenha apenas um único micro conectado à Internet, pode estar sujeito a ataques, sobretudo relacionados a vírus e trojans, já que a cada dia surgem novas dessas pragas virtuais, muitas delas indetectáveis pelos antivírus. Existem ainda possíveis bugs em aplicativos, que podem expor o seu micro a ataques. Por esse motivo, é indispensável que você atualize com freqüência o antivírus e demais aplicativos, principalmente os que utilizam a conexão com a Internet, incluindo o próprio sistema operacional. Se você utiliza alguma versão Windows, pode baixar atualizações através do Windows Update. Se você usa alguma distribuição Linux, verifique a disponibilidade de uma ferramenta de atualização de pacotes e mantenha-se atualizado com relação às atualizações disponibilizadas pelos desenvolvedores.

A partir do momento que se interliga os micros em rede e compartilha a conexão entre eles, os cuidados devem ser redobrados. Falhas nas configurações da rede ou mesmo desconhecimento por parte dos usuários podem tornar sua rede um prato cheio para os invasores. O risco é maior em redes corporativas e em sistemas bancários, onde o invasor pode obter vantagens mais diretas. Os scanners servem justamente para checar as condições de segurança de um ou mais micros, de modo que você corrija eventuais falhas antes que alguém mal intencionado tenha chance de explorá-las, obtendo alguma vantagem ou causando prejuízo. Assim como os demais, estes programas também precisam ser atualizados com frequência, de modo a corrigir falhas descobertas mais recentemente. Temos vários scanners disponíveis para download, alguns freewares, outros caríssimos. Entre os mais conhecidos e utilizados temos o Languard, o Project R3x e Shadow Security Scanner, todos eles bem recomendados. Na verdade, o R3x é mais antigo e deu lugar ao atual Languard Network Security Scanner, mas não deixa de ser uma ótima pedida, seja pela sua rapidez e leveza, seja pela eficiência em descobrir informações e compartilhamentos. Utilizá-los é bem simples. Uma vez instalados (com exceção do R3x que não necessita instalação), você define um endereço ou uma faixa de endereços IP e inicia a varredura. Este processo pode demorar um pouco, aumentando exponencialmente de acordo com o número de endereços a serem verificados. Se você possui uma rede, poderá checar as vulnerabilidades de todos os micros de uma só vez, indicando uma faixa contendo todos os endereços. Terminada a verificação, é

exibido um relatório contendo os resultados. O relatório não é difícil de se interpretar, mas para entendê-lo, você deve ter o mínimo de conhecimento sobre redes e protocolos, sobretudo com relação ao TCP/IP. Os resultados mais comuns são: portas abertas utilizadas por serviços de sistema, portas abertas por trojans e compartilhamentos de pastas, unidades de disco e impressoras. Caso você encontre alguma porta aberta e não exista nenhum serviço ou programa utilizando esta porta, sugiro que você a feche. Mas, claro, não saia por aí "fechando todas as portas", senão seu micro se tornará incomunicável e a melhor sugestão seria então, desconectá-lo da Internet. Muitos aplicativos precisam de determinadas portas para funcionar, como os compartilhadores de arquivos, por exemplo. Na verdade eles utilizam portas randômicas, ou seja, só são abertas durante o uso do programa. Se você instalar um programa deste tipo, nunca deixe o firewall bloqueá-lo, caso contrário o programa não conseguirá abrir a porta para que o seu correto funcionamento aconteça. Alguns scanners permitem salvar os relatórios obtidos em formato html, permitindo assim que você vá acompanhando os resultados obtidos a cada varredura efetuada. Isso é muito interessante, pois assim será possível verificar se as falhas encontradas nas varreduras passadas já foram corrigidas, ou se apareceu uma nova vulnerabilidade.

A Internet nada mais é do que a união de inúmeras sub-redes espalhadas pelo mundo, conectadas entre si. Essas sub-redes podem ser formadas por alguns ou vários micros conectados através de cabos e demais equipamentos de rede. Além destes dispositivos, que conectam fisicamente os micros, é necessário que cada micro da rede possua um protocolo comum instalado, como o TCP/IP, que é o protocolo padrão da Internet. É justamente o protocolo TCP/IP que permite que usuários de todo o mundo acessem sites, troquem informações, disputem jogos, entre tantos outros atrativos. E também é por esse mesmo protocolo que ataques hacker vindos de qualquer ponto do globo terrestre tornam-se possíveis. Um usuário que acessa a Internet de casa dificilmente estará vulnerável. O principal fator causador de ataques a usuários comuns é a **engenharia social**. Veja uma definição exata para o termo:

> "...práticas utilizadas para obter acesso à informações importantes ou sigilosas em organizações ou sistemas por meio da enganação ou exploração da confiança das pessoas. Para isso, o golpista pode se passar por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área, etc. É uma forma de entrar em organizações que não necessita da força bruta ou de erros em máquinas.

> Explora as falhas de segurança das próprias pessoas que, quando não treinadas para esses ataques, podem ser facilmente manipuladas." *(fonte: Wikipedia.org)*

Quando se trata de engenharia social, não há nenhum programa que possa corrigir a falha de segurança, já que ela não está no sistema e sim no próprio operador. A única sugestão neste caso é evitar executar programas vindos de pessoas e/ou sites desconhecidos e prestar atenção com aqueles links que aparentemente apontam para determinado destino mas que iniciam misteriosamente o download de algum arquivo (muito comum em sites de relacionamento, como o Facebook). Não só a engenharia social pode causar estragos, mas muitas vezes a própria falta de conhecimento ou treinamento por parte dos administradores de rede. Utilizar bons antivírus e firewalls nem sempre é suficiente, ainda mais quando estes não são atualizados. Pragas como trojans, que podem passar muitas vezes desapercebidas por antivírus, dificilmente não serão detectadas por um scanner. A grande vantagem em utilizá-lo, é justamente a possibilidade de se descobrir portas abertas, que podem ser causadas justamente pelos trojans. Talvez o programa não detecte a praga em si, mas certamente detectará a porta aberta por ela.

2.2.Sniffers

Os sniffers, conhecidos também como analisador de pacotes ou de rede, é o procedimento realizado por uma ferramenta, programas(software) ou adaptadores(hardware), com o intuito de interceptar e registrar todo o tráfego de informações que transitam em uma rede de computadores. De acordo com que o fluxo de dados passa na rede, o sniffer(analisador de pacotes) captura uma informação e logo decodifica(traduz para uma linguagem de entendimento) e faz uma análise do conteúdo desse pacote(informação).

O sniffing(analisador de pacotes) pode ser usado com intuito malicioso e também para gerenciamento da rede. Invasores podem também tentar capturar o tráfego da rede com inúmeros objetivos. Alguns desses objetivos são a cópia de arquivos importantes durante essa transmissão, obter senhas para aumentar o grau da invasão ou até mesmo ler conversações em tempo real.

2.2.1. Port Mirror – Port Spam – Port Monitor

Essa opção é desejável se o administrador da rede desejar conectar um sniffer(analisador de pacotes) uma porta só switch, para monitorar o tráfego das outras portas do equipamento. Ele deve definir qual porta será monitorada(port mirror) e o seu espelho, que é a porta onde o analisador de pacotes vai ser conectado. Uma vez que essa funcionalidade for ativa, todo o tráfego oriundo ou destinado à porta monitorada deverá ser monitorado por seu espelho.

2.2.2. Sniffers – Wireless

Existem diversos analisadores de protocolo que funcionam em conexões wireless. Algumas alterações nas configurações do analisador de protocolo em uso, talvez devam ser realizadas, como a habilitação da opção de captura em modo de monitoração, pois o modo promíscuo pode não ser suficiente. A captura ocorrerá da mesma maneira que ocorreria se estivesse numa conexão cabeada. O que pode ocorrer é alguma restrição do próprio sistema operacional que se está utilizando, bem como da interface de rede 802.11. A limitação de alguns sistemas operacionais é a de não capturar pacotes que não sejam de dados, o que ocorre também com alguns drivers dos adaptadores de rede.

É importante mencionar que o fato de uma interface de rede estar executando em modo de monitoração, nem sempre a habilitará a funcionar como uma interface de rede comum, pois ela estará capturando os pacotes em modo passivo. Com isso, as tentativas de resolução de nomes através de um servidor DNS, por exemplo, provavelmente estarão bloqueadas, pois o equipamento não estará habilitado para se comunicar com qualquer DNS Server.

2.3.DoS (Denial of Service) e DdoS (Distributed Denial of Service)

2.3.1. O que são ataques DoS?

Os ataques DoS (sigla para ***Denial of Service***), que podem ser interpretados como "Ataques de Negação de Serviços", consistem em tentativas de fazer com que computadores - servidores Web, por exemplo - tenham dificuldade ou mesmo sejam impedidos de executar suas tarefas. Para isso, em vez de "invadir" o computador ou mesmo infectá-lo com malwares, o autor do ataque faz com que a máquina receba tantas requisições que esta chega ao ponto de

não conseguir dar conta delas. Em outras palavras, o computador fica tão sobrecarregado que nega serviço.

Os ataques do tipo DoS mais comuns podem ser feitos devido a algumas características do protocolo TCP/IP (Transmission Control Protocol / Internet Protocol), sendo possível ocorrer em qualquer computador que o utilize. Uma forma de ataque bastante conhecida, por exemplo, é a SYN Flooding, onde um computador tenta estabelecer uma conexão com um servidor por meio de um sinal do TCP conhecido por SYN (Synchronize). Se o servidor atender ao pedido de conexão, enviará ao computador solicitante um sinal chamado ACK (Acknowledgement). O problema é que, em ataques deste tipo, o servidor não consegue responder a todas as solicitações e então passa a recusar novos pedidos. Outra forma de ataque comum é o UPD Packet Storm, onde um computador faz solicitações constantes para que uma máquina remota envie pacotes de respostas ao solicitante. A máquina fica tão sobrecarregada que não consegue executar suas funções. Menos frequente, outro exemplo de ataque explora falhas de segurança em softwares, especialmente sistemas operacionais (daí a importância de sempre mantê-los atualizados e protegidos com ferramentas de segurança). Neste tipo, um atacante pode rastrear a rede à procura de máquinas vulneráveis e enviar a elas pacotes que, por alguma razão, fazem o sistema interromper sua atividade.

2.3.2. O que são ataques DDoS?

DDoS, sigla para ***Distributed Denial of Service***, é um tipo de ataque DoS de grandes dimensões, ou seja, que utiliza até milhares de computadores para atacar uma determinada máquina, distribuindo a ação entre elas. Trata-se de uma forma que aparece constantemente no noticiário, já que é o tipo de ataque mais comum na internet. Para que ataques do tipo DDoS sejam bem sucedidos, é necessário que se tenha um número grande de computadores para que estes façam parte do "exército" que participará da ação. Uma das melhores formas encontradas para se ter tantas máquinas foi a de inserir programas de ataque DDoS em vírus ou em softwares maliciosos.

Inicialmente, organizadores de ataques DDoS tentavam "escravizar" computadores que agiam como servidores na internet. Entretanto, com o aumento constante na velocidade de acesso à internet por causa das conexões banda larga, passou-se a existir interesse pelos computadores dos usuários domésticos, já que estes representam um número extremamente grande de máquinas e, muitas vezes, podem ser "escravizados" mais facilmente. Nesta forma

de ataque, é comum o uso de computadores domésticos, já que estes são maioria e, muitas vezes, não são devidamente protegidos. Assim, é mais fácil infectá-los com um *malware* que possui instruções para fazer com que a máquina participe de um ataque DDoS. Quando o computador passa a fazer parte de uma botnet, esta máquina pode ser chamado de "zumbi". Após a contaminação, os "zumbis" podem entrar em contato com máquinas "mestres", que por sua vez recebem orientações (quando, em qual site/computador, tipo de ataque, entre outros) de um computador "atacante" ou "líder".

Um computador "mestre" pode ter sob sua responsabilidade até milhares de computadores. Repare que, nestes casos, as tarefas de ataque DoS são distribuídas a um "exército" de máquinas "escravizadas", fazendo jus ao nome ***Distributed Denial of Service*** (Negação de Serviço Distribuído). A imagem abaixo ilustra a hierarquia de botnets em ataques DDoS:

Figura 1 - InfoWester - Ataque DoS e DDoS (http://www.infowester.com/ddos.php)

2.4.Trojans

O Cavalo de Tróia ou Trojan Horse é um tipo programa malicioso que podem entrar em um computador disfarçados como um programa comum e legítimo. Ele serve para possibilitar a abertura de uma porta de forma que usuários mal intencionados possam invadir seu PC. Seu nome surgiu devido à história da guerra de Tróia e que culminou com a destruição desta. O cavalo de Tróia, um grande cavalo de madeira, fora supostamente

oferecido como um pedido de paz por parte dos gregos. Sendo um presente para o rei, os troianos levaram o cavalo para dentro das muralhas da cidade.

Os dois tipos mais comuns de Trojans são os Keyloggers (que normalmente são utilizados para roubar senhas) e os Backdoors (arquivos que possibilitam aberturas de portas para invasão). Diferente dos Vírus e Worms, eles normalmente não se auto copiam, não necessitam infectar outros programas para executar suas funções: eles são autônomos necessitando apenas ser executados, costumam instalar-se com arquivos que quando apagados podem gerar perda de dados.

Como eles são menos limitados podem ser potencialmente mais perigosos e as vezes não são identificados como ameaças. Assim, como uma forma de prevenção, arquivos executáveis desconhecidos ou de origem duvidosa, ainda que não sejam acusados como ameaças pelos antivírus, devem ser executados com cautela.

3. CONCLUSÃO

A segurança da informação tem um papel fundamental para as organizações, impactando direta e indiretamente no negócio da empresa e minimizando os riscos. Devido a isto, realizar um teste de invasão na infra-estrutura de TI é de suma importância que deve incluído nas políticas de segurança da informação interna, lembrando que devem-se seguir todas as etapas do teste de invasão para que os resultados sejam obtidos com sucesso.

O artigo apresentou algumas técnicas e métodos usados por pessoas mal intencionadas para conseguir invadir sistemas computacionais, porém segurança é vista mais amplamente, com diversas outras ferramentas, técnicas e até mesmo pessoas que podem ser abordadas para atingir resultados positivos ou negativos em muitas vezes.

É sempre importante observar e também realizar auditorias preventivas na rede, para que o negócio da empresa não seja afetado, evitando assim fraudes internos e externos. Vale salientar que o aprofundamento desta pesquisa se deu graças ao conhecimento de pessoas mais experientes, como o orientador do artigo, com sua vasta experiência na área de tecnologia, sendo uma peça fundamental para o aproveitamento do trabalho, o qual soube me guiar e direcionar para atingir a meta proposta.

4. REFERÊNCIAS

PEREIRA, A ndré L. Grupo hacker AntiSec divulga dados de 1 milhão de usuários da Apple, 2012. Disponível em: <http://www.tecmundo.com.br/ataque-hacker/29446-grupo-hacker-antisec-divulga-dados-de-1-milhao-de-usuarios-da-apple.htm> Acesso em: 04 de novembro de 2016.

WADLOW, Thomas A. Segurança de redes: projeto e gerenciamento de redes seguras. Tradução: Fábio Freitas da Silva. Rio de Janeiro: Campus, 2000.

WACK, John; TRACY, Miles; SOUPPAYA, Murugiah. NIST -SP800-42: Guideline on Network Security Testing. Washington: Natl, Inst. Stand. Technol. Espec., 2003

DIAS, Cláudia. Segurança e Auditoria da Tecnologia da Informação. AxcelBooks. Rio de Janeiro, 2000.

BRITO, Nelson. Protocol T50 5.3. Web Security Forum. April, 2011. Disponível em: <http://t50.sourceforge.net/resources.html> Acesso em: 04 de novembro de 2016.

NMAP. Network Mapper. Disponível em: <https://nmap.org/> Acesso em: 04 de novembro de 2016.