Introdução à Engenharia Social

Apresentar umas das técnicas utilizadas pelos invasores para obter dados e informações das empresas sem a utilização de tecnologia, apenas utilizando-se de uma fraqueza das políticas de segurança da informação que está atrelada ao não envolvimento do fator humano no processo da segurança.

Engenharia Social

Introdução

Nada mais é do que a técnica que o invasor se utiliza para conseguir, por meio da manipulação dos relacionamentos das pessoas, informações que utilizará para o seu processo de invasão, sem que para isso tenha de se utilizar de meios eletrônicos ou outros dispositivos físicos. Mas ele faz isso com a ajuda inconsciente das pessoas.

Como a segurança se baseia na confiança, as informações conseguidas pelo invasor são obtidas na maioria das vezes em virtude da grande ingenuidade e "falta de conhecimento" dos envolvidos ou pela confiança que essas pessoas tinham no invasor.

Vimos na aula 9 os conceitos de VLAN e suas características. Uma das principais funções de uma VLAN é proporcionar uma segmentação de rede LAN e melhor gerenciamento dela.

Só que, para isso ocorrer, é necessário um equipamento específico: o switch.

Existem atualmente no mercado diversos modelos e complexidades de switch. Por padrão, os switches são elementos pertencentes à camada 2 do modelo OSI, pois suas características típicas são os trabalhos com endereçamento MAC.

Mas, para que se possa proporcionar um melhor gerenciamento das segmentações de LANs, esses switches precisam de funções mais específicas. É aí que grandes fabricantes, como a Cisco, disponibilizam no mercado modelos de switches conhecidos como switches de multicamada, que, além de propiciarem todo o controle da camada 2, também apresentam controles de gerenciamento da camada 3 do modelo OSI.

Existem ainda alguns modelos mais avançados que permitem trabalhos com protocolos pertencentes à camada 4 do modelo OSI.

A seguir, apresentaremos o funcionamento básico desses switches.

Funcionamento

O invasor faz uso de suas habilidades para obter informações ou acesso indevido a determinado ambiente ou sistema, com a utilização de técnicas de persuasão que acabam na maioria das vezes resultando em informações chaves que poderão ser utilizadas por ele nos seus ataques.

As informações coletadas pelo invasor poderão ser os nomes de funcionários, estrutura de funcionamento da empresa, horário de entrada de pessoas e equipes de manutenção, softwares adquiridos, equipes que estão realizando algum tipo de treinamento, versão do Sistema operacional, entre outras informações.

O foco principal é obter informações que facilitarão o acesso dele à organização alvo. Conforme o que foi exposto anteriormente, fica bem evidente que para cometer esse tipo de ataque não são necessárias a utilização de ferramentas caras, mas sim a realização de ações altamente eficazes, com custo relativamente reduzido.

A engenharia social é considerada um dos meios mais utilizados para obtenção de informações sigilosas e importantes, hoje em dia, dentro das organizações.

Pelo fato de as empresas estarem preocupadas com o seu negócio e com a competitividade junto aos seus concorrentes, cada vez mais elas investem em tecnologias de ponta visando se proteger de ataques de hackers e suas variantes.

É investido muito dinheiro com o intuito de buscar identificar o melhor software, o melhor antivírus, o melhor firewall o melhor controle de acesso físico e lógico. Alem disso, são realizadas pesquisas de novas tecnologias para bloquear e contra-atacar uma possível invasão. No entanto, as empresas acabam por deixar de lado o fator humano, que corresponde na maioria das vezes ao ponto mais vulnerável desse processo de ataque pelo engenheiro social.

Os novos switches do mercado possuem uma capacidade extra. Além de trabalharem na camada 2 do modelo OSI como qualquer switch, também trabalham na camada 3, examinando o pacote IP que está encapsulado no frame Ethernet e tomando decisões de comutação baseadas nessa informação. Esses switches são também chamados de IP switches ou Routing Switches (roteadores) e em geral trabalham de forma muito parecida com um roteador.

Quando um switch é multicamadas, além de analisar o endereço IP para

tomar a decisão de comutação, analisa a porta TCP do pacote IP encapsulado no frame Ethernet – então dizemos que é um switch camada 4.

Quanto à forma de segmentação das sub-redes, podem ser classificadas como:

- Switches de camada 2
- Switches de camada 3
- Switches de camada 4

- Switch da camada 2 (enlace): são os switches tradicionais, que efetivamente funcionam como bridges multiportas. Sua principal finalidade é dividir uma LAN em múltiplos domínios de colisão. Esses switches trabalham apenas com o endereço MAC.

- Switch da camada 3 (rede – endereçamento): são os switches que, além das funções tradicionais da camada 2, incorporam algumas funções de roteamento, como a determinação do caminho de repasse baseado em informações de camada de rede e endereço do IP.

- Switch da camada 4 (transporte): basicamente incorpora às funcionalidades de um switch de camada 3 a habilidade de se implementar a aplicação de políticas e filtros de tráfego a partir de informações da camada 4 ou superiores.

Diferenças entre switch camada 2 e switch camada 3

Os switches de camada 3 também são comumente chamados de switch "layer" 3. Portanto, toda vez que uma bibliografia trata o switch como "layer" 2 ou "layer" 3, isso nada mais significa que switch de camada 2 ou switch de camada 3.

Um outro item importante que deve ser observado é quanto às características físicas de um switch. Se quisermos classificar um switch como camada 2 ou camada 3, apenas visualizando uma imagem ou o próprio equipamento, isso dificultará bastante, porque o switch, por se tratar de um comutador, apresenta as mesmas características físicas se comparados um ao outro.

A característica mais importante que deve ser observada é com relação ao software gerenciador do equipamento, junto ao seu modelo, por exemplo, se for um equipamento da fabricante "Cisco", um modelo característico gerenciador é o "Catalyst 8500".

Em arquiteturas de redes simples o roteador acaba se tornando o Backbone da rede, provendo conexões a LANs, a servidores locais, a WAN e à internet, exercendo múltiplas funções.

O tráfego de dados proveniente da WAN e da internet tem aumentado a cada dia, exigindo cada vez mais do roteador e sobrecarregando-o; como consequência, cria-se nesse ponto um inevitável gargalo.

Para agravar ainda mais a situação, as empresas estão migrando para redes Fast Ethernet e os roteadores conseguem operar com pouco mais de meia dúzia de interfaces Fast Ethernet.

À medida que mais estações migram para Fast Ethernet, o Backbone precisa migrar para Gigabit Ethernet, para poder oferecer uma largura de banda adequada.

Atualizar os roteadores existentes para adequá-los ao aumento de tráfego da rede é oneroso e, em muitos casos, pode-se não alcançar o desempenho desejado. Isso leva a uma busca por novas soluções.

A ideia principal em um ataque de Engenharia Social é conseguir persuadir as pessoas (funcionários, colaboradores) para fornecerem informações não autorizadas para um possível atacante, sem o uso de qualquer agressão. Como no mundo físico, o atacante tentará driblar as barreiras físicas e se infiltrar de forma disfarçada dentro de um prédio após passar pelas suas barreiras de segurança. Para isso poderá obter informações que para muitos não significam nada, mas podem ser utilizadas de forma combinada com outras, e assim cria-se um conjunto de informações que pode ser usado para cometer o ataque.

Uma lista abandonada em uma lata de lixo contendo os nomes dos funcionários que têm o seu turno na portaria de um prédio aparentemente pode não significar nenhum perigo. No entanto, se junto a essa lista ainda houver outra com o nome dos funcionários da empresa, ela poderá ser usada por um atacante. Com base nessas informações o atacante poderá convencer um vigia que se trata de um funcionário que trabalha no turno da noite e que acabou esquecendo o seu crachá. Ao chamar o vigilante pelo nome, já passa a falsa impressão que existe uma relação profissional entre eles, intimidando o vigia a ser mais rigoroso. Basta agora associar informações que por ventura também possam ter sido encontradas no lixo e que revelem outras sobre esse vigia, e tudo estará resolvido.

O engenheiro social

Exemplos de produtos de roteamento de alta velocidade são: Bay Networks Accelar, Cabletron SmartSwitch™ Router, Cisco Systems Catalyst 8500, Extreme Networks Summit, Foundry Networks Net/Turbo/BigIron Routers, Packet Engines PE-4884, Torrent Networking IP9000.

Os switches que utilizam essa tecnologia possuem uma taxa de transferência de dados mais alta que a dos roteadores tradicionais, já que não oferecem todas as funcionalidades disponibilizadas pelos roteadores. Enquanto os roteadores podem operar como backbone de redes e dispositivos de acesso à WAN e à internet, os novos switches, apesar de processarem o roteamento IP, só possuem interfaces LAN, não realizando conexões com a WAN ou com a internet.

O novo switch camada 3, também chamado de acelerador de roteador, é o resultado da combinação do switch camada 2 (que opera com MAC address) com o roteamento IP da camada 3, que controla o tráfego local que iria direto para o roteador. Utilizando a tecnologia das bridges de guardar endereços e aprendendo a localização do endereço IP nas várias portas, esse switch monta dinamicamente sua própria tabela de roteamento, utilizando essas informações para selecionar os dados que serão enviados ao roteador.

Os dados que realmente precisam ser manipulados pelo roteador é que são enviados, mas na

maioria dos casos os dados podem ser simplesmente enviados à sub-rede apropriada, tarefa que passa a ser executada pelo switch. A diferença entre os switches camada 3 e os camada 2 é que o primeiro pode direcionar o tráfego de dados de forma inteligente, enquanto o segundo passa adiante todos os dados, sem examiná-los.

Combinando um roteador tradicional baseado em software com um switch camada 3, pode-se reduzir consideravelmente a carga de trabalho sobre o roteador e aumentar a taxa de transferência entre sub-redes para milhões de pacotes por segundo. Com esses switches as empresas podem manter o tráfego LAN a LAN fluindo, com um custo menor do que repor os roteadores existentes.

Vale lembrar que o tráfego de dados que requer transporte por meio da WAN ou que não seja baseado em IP (IPX™, AppleTalk®, DECnet™) precisa passar pelo roteador, uma vez que o Switch camada 3 manipula apenas transmissões IP, e não suporta multiprotocolos nem interface WAN.

Agora que você já estudou esta aula, resolva os exercícios e verifique seu conhecimento. Caso fique alguma dúvida, leve a questão ao Fórum e divida com seus colegas e professor.

objeto disponível apenas na versão web

Desde os ataques de 11 de setembro e também por causa das leis e regulamentações nacionais e internacionais às quais as organizações financeiras ficaram sujeitas, ficou muito difícil de os atacantes da internet conseguirem acesso às informações dessa organização. Dessa forma o meio mais fácil e mais barato seria que esses criminosos tentassem enganar as pessoas que pertencem a essas organizações, de forma que elas fornecessem as informações necessárias para que ele burlasse as principais barreiras.

Antes do advento da internet, o atacante utilizava como ferramenta o telefone ou até mesmo o contato físico pessoal para obter as informações necessárias para o ataque ao seu alvo.

Hoje em dia uma simples pesquisa na internet atrás de informações sobre a instituição que será o alvo de ataque traz uma série de dados que podem ser utilizados para esse fim.

Exemplo de ataque de Engenharia Social

Muitas organizações já foram atacadas por técnicas de Engenharia Social e na grande maioria das vezes não têm conhecimento do fato, e provavelmente muitos segredos de negócio podem ter sido transferidos para seus concorrentes sem que a organização sequer suspeitasse que isso aconteceu.

Esse tipo de ataque tem êxito em organizações que não dão tanta importância para a parte humana envolvida no processo de segurança da informação. Essas organizações focam suas ações nas políticas e nas ferramentas de segurança e acabam não implementando a consciência coletiva em relação ao assunto segurança da informação.

Principais alvos da Engenharia Social

São os guardas; vigias; faxineiros; assessores de diretores importantes; estagiários; aprendizes, administradores de rede; usuários; secretárias e técnicos.

De maneira geral, qualquer ser humano está sujeito a um ataque de Engenharia Social, pois, no nosso dia a dia, quantas vezes já utilizamos essa técnica para obter informações de pessoas do nosso convívio social, apenas omitindo fatos ou falando parte da verdade para possuir ajuda na obtenção de informações secretas.

Técnicas mais usuais para o ataque de Engenharia Social

- Por meio de uma boa conversa, o atacante tentará ludibriar o envolvido de forma que ele passe as informações necessárias para o ataque.

- A ideia é o atacante convencer por meio da sua escrita o colaborador da empresa, para que este forneça informações sigilosas ao invasor sem que perceba fazer isso.

- O atacante força, de forma não perceptível, o colaborador a executar um programa ou código malicioso na máquina alvo para que posteriormente seja aberta uma porta de acesso remoto.

- Nesses locais o invasor aproveita para ganhar a confiança do colaborador e obter informações necessárias para o seu ataque.

- Novamente o invasor utiliza suas habilidades para convencer o colaborador a passar informações sensíveis da empresa.

- A análise do lixo pode trazer informações importantes para um ataque, como o número de máquinas da rede, servidores, roteadores, equipamentos de Access point, marca de equipamentos, suas versões, informações que ajudarão o invasor a identificar qual a melhor ferramenta para o seu ataque.

- Por meio de um link encaminhado para o colaborador, tenta forçar o colaborador a acessar uma página falsa de comércio eletrônico ou internet banking, fazendo-o digitar senhas ou códigos que poderão ser capturados e utilizados futuramente em processo de ataque.

- Nesse tipo de técnica, o invasor se aproveita do fato de uma pessoa não conhecer um determinado idioma ou de ela ter, por algum motivo, apertado as teclas do seu teclado em uma sequência incorreta, o que acabou apontando para o site falso.
- Esses sites falsos (clones) parecidos com o site verdadeiro são colocados em funcionamento e quando o colaborador pensa que navega no site desejado, na realidade navega no site do invasor, que se aproveita desse fato para capturar os dados do colaborador.

- Situações normais que qualquer ser humano tem, como a vontade de ser útil, de procurar sempre agir com cortesia ajudando os outros, a exploração desse tipo de vulnerabilidade pode possibilitar ao atacante conseguir as informações desejadas.

- Consiste na técnica de explorar a natureza humana, que possui diversos aspectos que podem ser manipulados por causa das necessidades básicas de aceitação, reconhecimento e motivação.

Cada uma dessas informações poderá servir como a primeira pedra na construção de um ataque à organização alvo. Hoje em dia uma grande fonte de informação para os engenheiros sociais dentro da internet são o Facebook e o Orkut, uma vez que esses sites permitem que as pessoas armazenem os seus dados pessoais, além de detalharem as suas atividades diárias, bem como a de seus amigos.

Dessa forma os engenheiros sociais não necessitam mais sair de suas casas, basta apenas navegar atrás das informações desejadas.

Como foi informado anteriormente, as empresas investem altas quantias de dinheiro em tecnologias de segurança que as ajudam a proteger fisicamente seus sistemas, porém não investem em treinamento seus funcionários, para protegê-los dessas terríveis armadilhas aplicadas pelos engenheiros sociais.

Para evitar esse tipo de ataque, algumas medidas deverão ser tomadas por parte dos responsáveis pela administração da segurança:

- A implementação de uma Política de Segurança na organização, bem como sua ampla divulgação, a conscientização dos funcionários com relação aos ataques de Engenharia Social e o que eles representam para a empresa poderão contribuir muito para que esse tipo de ataque não tenha sucesso.
- A implementação de dispositivos de segurança física e lógica, de forma a diminuir a possibilidade da entrada na empresa de conexões, sem que haja uma autenticação forte, como biometria ou smart cards, também pode ser uma recomendação para ajudar a segregar e proteger melhor esse ambiente,

- Monitoração constante de visitantes às instalações da empresa, bem como acompanhamento deles durante o desenvolvimento das suas atividades no interior da empresa, seja fisicamente ou por meio de dispositivos eletrônicos.
- Aplicação da política de mesa limpa e remoção de toda e qualquer informação classificada pela política de Classificação da informação, como forma de evitar deixar informações sensíveis ao alcance de potenciais invasores.
- Adoção de uma picotadora de papéis visando eliminar de forma correta as informações sensíveis em qualquer ambiente interno da empresa.
- Treinamento e orientação aos colaboradores da organização para não abrir e-mails de pessoas que não fazem parte do seu convívio diário dentro e fora da organização, principalmente as que solicitam a execução de uma ação potencialmente perigosa no seu computador.
- Monitoração das atividades dos estagiários e dos aprendizes que, por causa da sua falta de experiência, são frequentemente acessadas por parte desses atacantes, uma vez que eles se conectam na internet para conversar, baixar música, entrar em comunidades, e são nesses locais que tais golpistas costumam tentam achar uma brecha para poder aplicar o seu golpe.

Mesmo com o surgimento diário na internet de novas ferramentas para ataques automatizados, explorar a ingenuidade humana ainda é uma forma muito fácil, menos perigosa e que na maioria das vezes traz os resultados esperados, depois de se burlar de forma eficiente as seguranças das redes corporativas.

Muitos ataques de Engenharia Social são complicados e envolvem diversas etapas e planejamento elaborado, além de combinar o conhecimento da manipulação e tecnologia.

Geralmente a utilização de técnicas de Engenharia Social exige do atacante uma preparação psicológica muito grande para o momento do ataque, sendo que às vezes uma interação pessoal é necessária e ele deverá se preparar para enfrentar uma situação como essa.

O fato de tentar enganar uma pessoa pode parecer para muitos uma diversão ou algo intrigante, mas a aplicação dessa técnica é considerada como um crime e é passível de punição, que pode ir desde o pagamento de multas reais ou simbólicas à pena de detenção.

Esse tipo de ação, dependendo da gravidade que possa causar a alguma instituição, pode ser enquadrada como "falsidade ideológica", uma vez que uma mentira ou ação foi utilizada para cometer algum tipo de fraude.

Ataque direto e indireto

Podemos separar os ataques de Engenharia Social em dois tipos (direto ou indireto).

No primeiro tipo, o **direto**, existe o contato pessoal entre o atacante e o alvo, podendo ser realizado por meio de telefonemas, encontros físicos em palestras e congressos, e conforme informado anteriormente, o atacante deve se preparar psicologicamente para efetuar esse tipo de ataque.

No segundo tipo, o **indireto**, o ataque é realizado utilizando-se ferramentas de invasão específicas, que vão desde a utilização do Cavalo de Troia, ferramentas de monitoração, vírus, programas, keyloggers, screenlogger etc.

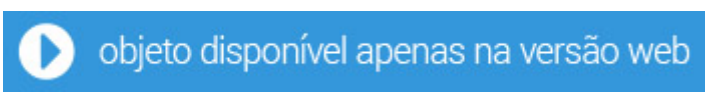
Outro aspecto interessante do engenheiro social é ele ser praticamente indetectável pelos sistemas tecnológicos das empresas, pois não deixa rastros que podem ser seguidos para a sua identificação.

Punições para os crimes de engenharia social

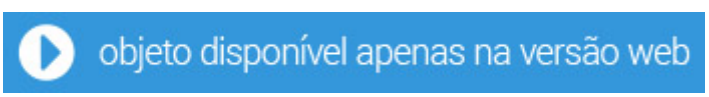
Aplicar uma punição para os responsáveis por ataques que utilizam técnicas de engenharia social pode ser considerada uma tarefa difícil, pois alguns desses ataque nem podem ser categorizados como crime uma vez que as informações obtidas haviam sido deixadas sem nenhuma proteção em cima de alguma mesa ou até mesmo descartadas dentro de um lixo que estava colocado do e do lado de fora da organização ou seja em um lugar público.

Agora que você já estudou esta aula, resolva os exercícios e verifique seu conhecimento. Caso fique alguma dúvida, leve a questão ao Fórum e divida com seus colegas e professor.

Agora que você já estudou esta aula, resolva os exercícios e verifique seu conhecimento. Caso fique alguma dúvida, leve a questão ao Fórum e divida com seus colegas e professor.



Para memorizar os conhecimentos adquiridos nesta aula, clique no botão a seguir e faça o caça-palavras proposto.



Estimule seu raciocínio com o jogo da forca, clique no botão a seguir.

Referências

ABNT – Associação Brasileira de Normas Técnicas. Tecnologia da Informação – Código de prática para a gestão de segurança da informação. NBR ISSO/IEC 17799: 2001. Rio de Janeiro.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. *Política de Segurança a Informação*: Guia Prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2006.

GOMES, José Anchieschi. *Segurança total*: protegendo-se contra hackers. São Paulo: Makron Books, 2000.

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. *Gerenciamento de Serviços de TI na Prática*: Uma abordagem com base na ITIL. São Paulo: Novatec, 2007.

MCCLURE, Stuart Scambray; SCAMBRAY, Joel; KURTZ, George. *Hackers expostos* – segredos e soluções para segurança de rede. São Paulo: Makron Books, 2000.

SÊMOLA, Marcos. *Gestão da Segurança da Informação*: Uma visão executiva. Rio de Janeiro: Elsevier, 2003.

WADLOW, Thomas A. *Segurança de redes*: projeto e gerenciamento de redes seguras. Rio de Janeiro: Campus, 2001.