Palestra de Segurança da Informação:

1. Quem Somos:

Slide: 2-3.

1.1: Yan Esteves.

- Sistemas de Informação - Faculdade Universo. - Desenvolvedor Web / Desktop.- Ex-Hacker. Especialista em Seg. Informação: Técnicas de Invasão, Udemy.

1.2: Eduardo Alexandre.

Sistemas de Informação - Faculdade Universo

Tecnologo in ADS - Faculdade Estácio Juiz de Fora , Téc.Química e Gestão Ambiental – Cetepro, Téc.Meio Ambiente – IFSMG, Téc.Redes de Computadores e Servidores - Senac Juiz de Fora.

Especialista em Seg.Informação in: Técnicas de Invasão(Guardweb), Udemy, Desec Security, Developer Full Stack.

2. Introdução:

Slide 4-5.

2.1: Conteúdos:

2.2: O que é ser Hacker?

Na informática, hacker é um indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores.

2.3: Nomenclatura Hacker:

- Hacker: Basicamente, hackers são indivíduos que possuem conhecimentos profundos na informática e que dedicam a maior parte do seu tempo a conhecer, modificar software, hardwares e redes de computadores.

- Cracker: Possui também grandes conhecimentos na informática, porém os utiliza de forma maléfica. O termo foi criado pelos próprios hackers em torno de 1985, por estarem cansados de serem chamados de criminosos virtuais e para que os leigos e a mídia soubessem distingui-los.

2.4: Grupos Hacker da Atualidade:

Anonymous: Anonymous é uma legião que se originou em 2003. Representa o conceito de muitos usuários de comunidades online existindo simultaneamente como um cérebro global. O termo Anonymous também é comum entre os membros de certas subculturas da Internet como sendo uma forma de se referir às ações de pessoas em um ambiente onde suas verdadeiras identidades são desconhecidas.

LulzSec: Lulz Security, abreviado por LulzSec, é um grupo ativista hacker responsável por ataques de alto perfil, incluindo o vazamento de dados de mais de 1.000.000 de contas de usuários da Sony em 2011. Declarou guerra aberta aos governos, bancos e grandes corporações em parceria com o Anonymous.

2.5: Hackers Da atualidade:

Edward Snowden é um analista de sistemas, ex-administrador de sistemas da CIA e ex-contratado da NSA que tornou públicos detalhes de vários programas que constituem o sistema de vigilância global da NSA americana.

3. Desenvolvimento:

3.1: Ferramentas:

Kali Linux: Algumas ferramentas do Kali Linux:

- Metaspoit: O **Metasploit** é uma ferramenta extremamente poderosa, voltada para **testes de invasão** (pentests), com ela é possível fazer desde um simples **scan**, até uma invasão completa, explorando vulnerabilidades no sistema operacional ou em programas que estejam instalados no computador alvo. Para isso o Metasploit conta com vários **exploits** e **módulos auxiliares**, além de alguns complementos.

- Aircrack: **Aircrack-ng** é um detector de redes, sniffer de pacote, aplicativo de quebra de WEP, WPA, WP2 e ferramenta de análise para redes locais sem fios 802.11. Funciona com qualquer placa wireless cujo driver suporta modo de monitoramento bruto (para uma lista, visite o website do projeto) e pode capturar e analisar (sniff) tráfego 802.11a, 802.11b e 802.11g.

SET: O Social Engineering Toolkit é uma ferramenta integrada com o Metasploit Framework com o objetivo de facilitar os testes, avaliações e ataques relacionados à engenharia social. Mesmo que você não tenha vocação hacker, é interessante conhecer a ferramenta para ver o quão simplesmente se realiza ataques hoje em dia.

NMAP: O Nmap("Network Mapper") é um ferramenta de segurança usada para detectar computadores e serviços numa rede, criando um "mapa" dessa mesma rede rede. O Nmap utiliza inúmeras técnicas de detecção. Para cada umas das técnicas de detecção, gera uma assinatura e uma expressão da reacção do sistema alvo à técnica de detecção usada. Como são utilizadas várias técnicas, são geradas várias assinaturas.

Maltego: O Maltego é um programa que recolhe informações de varias fontes publicas conhecido como "Open-source intelligence" e relaciona os dados recolhidos. Tem varias vertentes desde as analises de DNS como engenharia social, passando por um excelente relacionamento dos dados.

Tails OS: **Tails** é um sistema live que tem como objetivo preservar sua privacidade e anonimato. Ele te ajuda a utilizar a Internet de forma anônima e evitar a censura em praticamente qualquer lugar e qualquer computador sem deixar rastros, a não ser que você explicitamente peça que ele o faça.

3.2: Engenharia Social:

A **engenharia social**, no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais. Este é um termo que descreve um tipo psicotécnico de intrusão que depende fortemente de interação humana e envolve enganar outras pessoas para quebrar procedimentos de segurança. Um ataque clássico na engenharia social é quando uma pessoa se passa por um alto nível profissional dentro das organizações e diz que o mesmo possui problemas urgentes de acesso ao sistema, conseguindo assim o acesso a locais restritos.

3.2.1: Entendendo a engenharia social:

A engenharia social é aplicada em diversos setores da segurança da informação, e independentemente de sistemas computacionais, software e/ou plataforma utilizada, o elemento mais vulnerável de qualquer sistema de segurança da informação é o ser humano, o qual possui traços comportamentais e psicológicos que o torna suscetível a ataques de engenharia social. Dentre essas características, pode-se destacar:

A engenharia social não é exclusivamente utilizada em informática. Ela também é uma ferramenta que permite explorar falhas humanas em organizações físicas ou jurídicas as quais operadores do sistema de segurança da informação possuem poder de decisão parcial ou total sobre o sistema, seja ele físico ou virtual. Porém, deve-se considerar que informações tais como pessoais, não documentadas, conhecimentos, saber, não são informações físicas ou virtuais, elas fazem parte de um sistema em que possuem características comportamentais e psicológicas nas quais a engenharia social passa a ser auxiliada por outras técnicas como: leitura fria, linguagem corporal, leitura quente. Esses termos são usados no auxílio da engenharia social para obter informações que não são físicas ou virtuais, mas sim comportamentais e psicológicas.

3.2.2: Tecnicas:

A maioria das técnicas de engenharia social consiste em obter informações privilegiadas enganando os usuários de um determinado sistema através de identificações falsas, aquisição de carisma e confiança da vítima. Um ataque de engenharia social pode se dar através de qualquer meio de comunicação. Tendo-se destaque para telefonemas, conversas diretas com a vítima, e-mail e WWW. Algumas dessas técnicas são:

Vírus que se espalham por e-mail:

Criadores de vírus geralmente usam e-mail para a propagar as suas criações. Na maioria dos casos, é necessário que o usuário ao receber o e-mail execute o arquivo em anexo para que seu computador seja contaminado. O criador do vírus pensa então em uma maneira de fazer com que o usuário clique no anexo. Um dos métodos mais usados é colocar um texto que desperte a curiosidade do usuário. O texto pode tratar de sexo, de amor, de notícias atuais ou até mesmo de um assunto particular do internauta. Um dos exemplos mais clássicos é o vírus I Love You, que chegava ao e-mail das pessoas usando este mesmo nome. Ao receber a mensagem, muitos pensavam que tinham um(a) admirador(a) secreto(a) e na expectativa de descobrir quem era, clicavam no anexo e contaminam o computador. Repare que neste caso, o autor explorou um assunto que mexe com qualquer pessoa. Alguns vírus possuem a característica de se espalhar muito facilmente e por isso recebem o nome de worms (vermes). Aqui, a engenharia social também pode ser aplicada. Imagine, por exemplo, que um worm se espalha por e-mail usando como tema cartões virtuais de amizade. O internauta que acreditar na mensagem vai contaminar seu computador e o worm, para se propagar, envia cópias da mesma mensagem para a lista de contatos da vítima e coloca o endereço de e-mail dela como remetente. Quando alguém da lista receber a mensagem, vai pensar que foi um conhecido que enviou aquele e-mail e como o assunto é amizade, pode acreditar que está mesmo recebendo um cartão virtual de seu amigo. A tática de engenharia social para este caso, explora um assunto cabível a qualquer pessoa: a amizade.

3.3: Principais ataques:

3.3.1: DDOS Atack:

Um ataque de negação de serviço (também conhecido como DoS Attack, um acrônimo em inglês para Denial of Service), é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Alvos típicos são servidores web, e o ataque procura tornar as páginas hospedadas indisponíveis na WWW. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga. Os ataques de negação de serviço são feitos geralmente de duas formas:

- Forçar o sistema vítima a reinicializar ou consumir todos os recursos (como memória ou processamento por exemplo) de forma que ele não possa mais fornecer seu serviço;

- Obstruir a mídia de comunicação entre os utilizadores e o sistema vítima de forma a não se comunicarem adequadamente.

3.3.2: Cavalos de troia e outros:

O malware cavalo de Troia recebe esse nome devido a clássica história do cavalo de Troia, pois ele imita a técnica de infectar computadores. Um cavalo de Troia se ocultará em programas que parecem inofensivos, ou tentará enganá-lo para que você o instale.

3.3.3: Port Scanning Attack:

O atacante faz um escaneamento das portas do servidor atrás de falhas para poder atacar.

3.3.4: Ataques de Força Bruta

Os ataques de força bruta são ataques demorados capazes de quebrar senhas.

3.4: Eleições no Brasil:

O professor da Universidade Estadual de Campinas (Unicamp) Diego de Freitas Aranha coordenou uma equipe de profissionais num teste de segurança promovido pelo Tribunal Superior Eleitoral (TSE) em 2017. A missão deles, mostrar possíveis falhas no sistema de votação eletrônica adotado no Brasil, foi concluída com êxito.

O especialista foi um dos convidados da audiência pública realizada pela Comissão de Constituição, Justiça e Cidadania, nesta terça-feira (6), sobre segurança do voto eletrônico e implementação do voto impresso nas eleições gerais de 2018.

- No último dia de testes tivemos progressos. Conseguimos, por exemplo, alterar mensagens de texto exibidas ao eleitor na urna para fazer propaganda a um certo candidato. Também fizemos progresso na direção de desviar voto de um candidato para outro, mas não tivemos tempo de testar esse tipo de ataque - explicou.

Segundo Diego, a equipe dele trabalhou em condições piores do que trabalhariam verdadeiros fraudadores, devido a restrições técnicas e de tempo impostas pelo tribunal, mas ainda assim foi possível explorar pontos vulneráveis para adulterar o software de votação e entrar no ambiente da urna eletrônica.

Segundo o professor da Unicamp, o resultado não foi surpresa, visto que todo software é potencialmente vulnerável. Por isso, é importante o registro físico para que a escolha do eleitor seja resguardada de outra forma.

- Esse é um entendimento da comunidade técnica internacional e segue a experiência de outros países. Não há país no mundo que tenha migrado para a votação eletrônica que não use o registro

físico do voto como mecanismo de transparência. O registro físico é inegociável. É um instrumento básico de transparência - afirmou.

Professor lembrou que há cinco anos participou de testes semelhantes feitos pelo TSE. E na ocasião a equipe dele elaborou um ataque que quebrava o sigilo dos votos.

- Demonstramos que era possível recuperar os votos da urna em ordem, sabendo exatamente como votaram o primeiro, o segundo, o terceiro eleitores e assim sucessivamente - explicou.

3.5: Google Hack:

Google utiliza uma tecnologia chamada **spiders**, ou **webcrawlers** que são robôs que fazem a varredura na web buscando e** indexando as páginas**. Quando fazemos uma busca pela ferramenta ela procura por este termo nestas páginas indexadas nos retornando **o que estamos procurando de fato**, cada resultado retornado é composto por um **titulo**, uma **url** e uma **descrição**. Um servidor mal configurado pode expor informações da empresa no Google. Não é difícil conseguir acesso a arquivos de base de dados através do Google. O **Google Hacking** nada mais é que uma prática para encontrar aquivos e/ou falhas a partir do Google, usando ele como uma espécie de scanner, dando comandos e possibilitando manipular buscas avançadas por strings chamadas de “dorks” ou “operadores de pesquisa”.