Hacker? Como assim?

Vamos iniciar o curso elucidando conceitos por trás da palavra hacker, documentários sobre a origem da palavra e sua evolução como comunidade. Tenha em mente que a comunidade hacker sempre teve forte influência no desenvolvimento tecnológico. Começaremos entendendo mais sobre essa comunidade, para isso uma série de vídeos serão disponibilizados aqui.

https://www.youtube.com/watch?v=cgI1pesO1do

https://www.youtube.com/watch?v=3ctQOmjQyYg

https://www.youtube.com/watch?v=ZwLdB7Dblpw

Sistema Operacional Linux Kali

O Kali é uma reconstrução completa do BackTrack Linux, que adere totalmente aos padrões de desenvolvimento do Debian. Uma infraestrutura completamente nova foi montada, todas as ferramentas foram revistas e empacotadas, e nós utilizamos Git como nosso Sistema de Controle de Versões.

- Mais de 300 ferramentas de testes de intrusão: Depois de rever cada ferramenta que estava incluída no Backtrack, eliminamos um grande número de ferramentas que não funcionavam, ou para as quais havia outra ferramenta com funcionalidade semelhante.

- É, e sempre será gratuito: Kali Linux, como seu predecessor, é completamente livre, e sempre permanecerá como tal. Você nunca, nunca terá que pagar pelo Kali Linux.

- Repositório Git livre: Somos proponentes convictos do software de código aberto e nosso repositório está disponível para todos que todos vejam e todos os fontes estão disponíveis para aqueles que desejem adaptar e remontar os pacotes.

- Complacente com o padrão FHS: Kali foi desenvolvido para aderir ao Padrão Hierárquico do Sistema de Arquivos (ou FHS da sigla em inglês), permitindo que todos os usuários Linux facilmente localizem arquivos binários, de apoio, bilbiotecas, etc.

- Vasto suporte à dispositivos wireless: Construímos o kali Linux para suportar tantos dispositivos wireless quanto pudemos, permitindo que o mesmo executasse adequadamente numa vasta gama de hardware e o tornando compatível como diversos outros dispositivos sem fio e USB.

- Kernel adaptado para injeção de pacotes: Como consultores de testes de intrusão, a equipe de desenvolvimento às vezes precisa fazer avaliações em redes sem fio, então nosso kernel já inclui os últimos patches de injeção de pacotes.

- Ambiente de desenvolvimento seguro: A equipe do Kali Linux é formada de um pequeno grupo de pessoas de confiança as quais só podem submeter pacotes e interagir com os repositórios usando múltiplos protocolos de segurança.

• **Repositórios e pacotes com assinaturas GPG:** Todos os pacotes do Kali são assinados por cada desenvolvedor individual quando eles são construídos e submetidos ao repositório, que em seguida assina os pacotes também.

• **Múltiplos idiomas:** Embora as ferramentas usadas em testes de intrusão tendam a ser escritas em inglês, nós nos asseguramos que o Kali possuísse um suporte a idiomas real, permitindo que mais usuários o operassem no seu idioma nativo, e encontrasse as ferramentas de que precisa para realizar suas tarefas.

• **Totalmente customizável:** Nós entendemos perfeitamente que nem todos irá concordar com nossas decisões de design, então tornamos o mais fácil possível que nossos usuários mais aventureiros to customizem o Kali Linux ao seu gosto, através de todo o sistema até o kernel.

• **Suporte à ARMEL e ARMHF:** Já que os sistemas baseados em processadores ARM estão se tornando mais e mais presentes e baratos, sabíamos que o suporte a processadores ARM no Kali precisaria ser o tão robusto quanto pudéssemos gerenciar, o que resultou em instaladores funcionais tanto para sistemas ARMEL quanto para ARMHF. Kali Linux tem repositórios ARM integrados com a distribuição principal, então ferramentas para ARM serão atualizadas em conjunto com o resto da distribuição. Kali atualmente está disponível para os seguintes dispositivos ARM:

- rk3306 mk/ss808
- Raspberry Pi
- ODROID U2/X2
- Samsung Chromebook

O Kali é especialmente indicado para testes de intrusão, então toda a documentação deste site pressupõe um conhecimento anterior do sistema operacional Linux.

FONTE: http://br.docs.kali.org/introduction-pt-br/o-que-e-o-kali-linux

Lista de Comandos do Kali Linux: https://www.cybrary.it/0p3n/kali-linux-commands-list/

Obtendo Informações

Nesse capítulo iniciaremos a fase de coleta de informação do teste de invasão. O objetivo dessa fase é conhecer o máximo possível os nossos clientes, o CEO revela informações demais no Facebook? O administrador do sistema está escrevendo para Fóruns perguntando a respeito de como garantir a segurança de uma instalação em Wordpress? Quais softwares estão sendo executados em seus servidores Web? Os sistemas voltados à internet estão ouvindo mais portas do que deveriam? Ou se este é um teste de invasão interno qual é o endereço de IP do controlador de domínio? Também começamos a interagir com os nossos sistemas-alvo, conhecendo o máximo que pudermos sobre eles sem atacá-los de forma ativa. Usaremos o conhecimento adquirido na sua fase para prosseguirmos

para a fase de modelagem de ameaças em que pensaremos como os invasores, desenvolveremos planos de ataques com base nas informações coletadas. De acordo com as informações que descobrimos iremos procurar e verificar as vulnerabilidades de forma ativa usando técnicas de scanner de vulnerabilidades que serão discutidos nos próximos capítulos.

Netcraft

As informações que os servidores web e empresas de web hosting reúnem (e tornam publicamente disponíveis) podem dizer muito a respeito de um site. Por exemplo uma empresa chamada Netcraft faz log do uptime e consultas sobre o software subjacente. Essas informações estão publicamente disponíveis em www.netcraft.com, esse domínio também provê outros serviços.

Suas ofertas relacionadas ao anti-phishing são de particular interesse para a segurança da informação. O resultado ao fazer uma consulta em netcraft.com a procura de "http://londrina.pr.gov.br" traz algumas informações interessantes. O site da prefeitura de Londrina foi inicialmente visto em maio de 1998, possui o português como sua língua primária, endereço de IP 200.155.38.23 e um histórico de hospedagem bem detalhado, expondo também a tecnologia empregada na construção do site. Faça suas próprias consultas aqui: https://toolbar.netcraft.com/site_report?url=

Lookups com Whois

Todos os registradores de domínio mantêm registros dos domínios que eles hospedam. Esses registros contêm informações sobre os proprietários. Se executarmos a ferramenta de linha de comando "whois" em nosso computador Kali para solicitar informações sobre http://londrina.pr.gov.br como mostrado, veremos informações sobre o domínio, entretanto um registro privado não fornecera muitas informações.

Para a prática, utilize o Kali Linux e informe o comando "whois WEBSITE" em seu terminal.

Caso o "whois" não esteja instalado no linux utilize o comando "apt-get install whois" para proceder com a instalação do aplicativo.

A execução de consultas com o Whois em outros domínios mostrará resultados diferentes e consequentemente atrativos em um teste de invasão. Pode-se obter dados pessoais do responsável pelo registro como nome, telefone, cidade, e-mail, etc...

Nsookup

Também podemos usar servidores de DNS para reconhecer melhor um domínio, os servidores DNS traduzem a URL legível aos seres humanos em endereço IP, por exemplo podemos usar uma ferramenta de linha de comando como o "nslookup" conforme mostrado na figura. Também podemos usar a ferramenta para descobrir os servidores de e-mail para o mesmo site ao procurar registros MX (linguagem do DNS para e-mail).

O primeiro terminal exibe uma busca simples pelo domínio "londrina.pr.gov.br" que retorna o endereço de IP do servidor DNS. Através dos comandos:

~# nslookup

> set type=mx

> londrina.pr.gov.br

É possível identificar o servidor de e-mail atrelado ao domínio.

Host e Transferência de Zona

Outro utilitário para solicitar informações ao DNS é o "**host**" podemos pedir ao host que forneça os servidores de nome para um domínio por meio do comando "**host -t ns domínio**".

root@kali:~# host -t ns DOMÍNIO

Um Bom exemplo de consultas sobre domínio é o próprio site da prefeitura municipal de londrina londrina.pr.gov.br que está configurado para proceder com o recurso transferência de zona.

Insta salientar que a transferência de zona DNS é um recurso que quando não configurado corretamente propicia o vazamento das informações contidas na tabela do servidor DNS.

Essa saída mostra todos os servidores DNS de londrina.pr.gov.br, efetuaremos a demonstração de um ataque visando a transferência de zona em um servidor DNS.

A transferência de zona DNS permite que os servidores de nome dupliquem todas as entradas de domínio. Ao configurar servidores DNS normalmente você tem um servidor principal de nomes e um servidor backup. Não há melhor maneira de preencher todas as entradas do servidor DNS secundário do que consultar o servidor principal e solicitar todas as suas entradas, infelizmente muitos administradores de sistema configuram as transferências de zona DNS de forma não segura, permitindo que qualquer pessoa possa transferir registros DNS para um domínio. londrina.pr.gov.br é um exemplo, podemos usar o comando host para fazer o download de todos os registros DNS.

Utilize a opção **-l** para especificar o domínio a ser transferido e selecione um dos servidores de nome do comando anterior como mostrado na figura.

root@kali:~# host -l londrina.pr.gov.br ns.londrina.pr.gov.br

Existem várias páginas de entrada DNS para zoneedit.com o que nos dá uma boa ideia de onde procurar vulnerabilidades em nosso teste de invasão, por exemplo **gwmail.londrina.pr.gov.br** provavelmente é um servidor de e-mail, portanto devemos procurar softwares potencialmente vulneráveis que executem em portas típicas de e-mail, como a porta 25 e a porta 110.

Se pudermos localizar um servidor de Webmail, qualquer nome de usuário que encontrarmos poderá nos levar para a direção correta, visto a possibilidade de adivinhar senhas e obter acesso a e-mails que contenham dados críticos.

TheHarvester: Coleta de Informações

Testes de invasão externos com frequência encontram menos serviços expostos que testes de invasão internos, uma boa prática de segurança consiste em expor somente os serviços de acesso remoto essenciais como servidores web, o servidor de e-mail, os servidores VPN, e talvez, o SSH ou FTP em suma, os serviços que sejam críticos para a missão da empresa. Serviços como esses constituem superfícies comuns de ataque e a menos que os funcionários utilizem uma autenticação de dois fatores, acessar o webmail da empresa pode ser fácil se um invasor puder descobrir credenciais válidas.

Procurar endereços de e-mail na internet é uma maneira excelente de descobrir nomes de usuários, você ficaria surpreso ao encontrar endereços corporativos de e-mail listados publicamente em informações de contato em associações de pais e professores em listas de equipes esportivas e (é claro) em redes sociais.

Uma ferramenta Python chamada **TheHarvester** pode ser usada para analisar resultados de sites 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. Daremos uma olhada nos primeiros resultados das ferramentas de pesquisa.

Utilize o comando:

```
root@kali:~# theharvester options
```

... leia os parâmetros de uso do software, observe quais são as características de cada parâmetro (ex: **-d -l -b**).

Na prática podemos procurar endereços de e-mail informando qualquer website, para efeitos de teste o site da Universidade Estadual de Londrina (UEL) será consultado.

O comando:

```
root@kali:~# theharvester -d uel.br -l 200 -b all
```

Onde:

-d especifica o domínio a ser pesquisado

-l o limite dos resultados (200 resultados)

-b a fonte de dados utilizada (google, bing, pgp, etc.)

Observe na figura os primeiros emails encontrados pela ferramenta e tenha em mente que essa é apenas uma utilização básica do software.

Leve em consideração que o software não encontra apenas endereços de e-mail, em buscas avançadas podemos reconhecer servidores de ftp, ssh, http, entre outros. Grandes instituições caracterizam mananciais de informação para serem "mineradas".

Como exercício utilize opções de busca avançadas do TheHarvester em sua empresa ou website próprio e compare os resultados.

Maltego

O Maltego da Paterva é uma ferramenta para data mining ou 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 que usaremos neste curso limita os resultados retornados 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. Ao prestar serviços de pentest será necessário ter uma licença paga para executar o software, entretanto para vias de estudo, a versão disponível no Kali Linux é mais que suficiente.

Digite "maltego" no terminal, a interface gráfica do aplicativo deverá ser iniciada, posteriormente você será solicitado a criar uma conta gratuita no site da Paterva e fazer o login. Após o login selecione "abra um grafo em branco e deixe em brincar" e em seguida clique em "finalizar". Agora selecione a opção "paleta" na borda esquerda, note que podemos coletar informações sobre vários tipos de entidades.

Vamos começar com o domínio http://uel.br espanda as opções infra-estrutura na paleta e arraste uma entidade domínio para o novo grafo, por padrão o domínio é paterva.com, para alterar de 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 (que são uma linguagem do maltego para as consultas) instruindo o software a procurar informações interessantes. Vamos começar com algumas transformações simples que poderão ser visualizadas ao clicar com botão direito do mouse no ícone de domínio e selecionar executar transformações.

Maltego 101: What is Maltego? Haktip 109:

https://www.youtube.com/watch?v=wx4mEQZM_0s

Ip Logger

O Grabify é (assim como diversos outros sites do seguimento) um "registrador de IP's", isso quer dizer que quando criamos um link com o Grabify, certas informações dos usuários que acessarem esse link ficam armazenadas no site da ferramenta.

Ao criar um link você recebe uma chave de acesso para saber quantas e quais pessoas clicaram nesse link. Essa ferramenta constitui uma ótima oportunidade para coletar

informações acerca do endereço de IP, do sistema operacional e do browser utilizado pelo alvo.

Com isso em mente pode ser efetuado um ataque de engenharia social resultando em informações sobre o endereço de IP sistema operacional e browser utilizado pelos usuários que clicaram no link, como essas informações nós podemos iniciar um Scan de rede e de vulnerabilidades contra o endereço IP alvo, tópico futuro do curso.

Como é que isso funciona?

Digite uma URL que será o endereço final acessado pelo alvo (ex: um vídeo do Youtube, ou uma página no Facebook).

Forneça ao alvo o link gerado pelo Grabify (o Grabify é transparente ao alvo).

(Opcional): Utilize um encurtador de links para mascarar a utilização do Grabify.

Salve o código fornecido pelo site para poder consultar os indivíduos que clicaram posteriormente.

Posteriormente digite o código obtido através do Grabify para saber informações sobre quem clicou no seu link.

Google Hacking

Google hacking é uma técnica de hacking que usa o Google Search e outras aplicações do Google para encontrar falhas de segurança na configuração e nos códigos dos sites – Fonte: Wikipedia.

O Google é um sistema de busca muito poderoso e é capaz de fornecer muitas informações que são úteis para um hacker ou cracker. Usando Google dorks , é possível realizar diversos filtros e procurar por determinados sistemas ou configurações de aplicações. Por exemplo, o atacante pode extrair diversas informações como os detalhes de configuração de banco de dados, nome de usuário, senhas, listas de diretório, mensagens de erro, lista de emails, arquivos de backup, etc.

Um dos principais motivos de ocorrer esta exposição de dados é a falta de uma política de segurança relacionada aos servidores e dados que serão expostos na internet.

Existem alguns métodos que podemos utilizar para proteger os servidores que ficarão expostos na web.

Quando disponibilizamos um servidor público, normalmente esse servidor apenas armazena dados irrelevantes, que são na sua maioria, acessados pelo público em geral, mas se você está realmente preocupado de manter o acesso de alguns dados privados, então o melhor caminho é mantê-lo com acesso restrito.

Acredito que todos saibam sobre o risco associado com listagens de diretórios, o que permite usuário mal-intencionado visualizar a maioria dos arquivos armazenados dentro de um diretório, subdiretórios, etc. Algumas vezes até mesmo o arquivo .htaccess pode ser

listado, que normalmente é usado para proteger o conteúdo de um diretório de acessos não autorizados, mas um erro de configuração pode permitir que o arquivo seja listado e lido.

Quando um servidor possui dados importantes, onde existe a necessidade em permitir o acesso de qualquer lugar, esses dados podem ser indexados pelos crawlers dos buscadores. Uma das regras simples é que os administradores podem criar um arquivo chamado robots.txt, que especifica determinados locais, de modo que esses motores de busca não devem explorar e armazenar em cachê determinado site ou diretório.Por exemplo, para proteger um determinado diretório, podemos usar a seguinte configuração no robots.txt - User-agent: * Disallow: /documentos

Caso você deseje bloquear o acesso a páginas individuais ou se você deseja que qualquer página não seja indexada pelos mecanismos de busca, podemos utilizar os meta tags como - , que irá prevenir os robots de verificar os links de um determinado site.

Maiores informações sobre robots e meta tags podem ser obtidas no endereço http://www.robotstxt.org

Neste caso acima, citamos apenas o exemplo do uso dos robots.txt, porém, o Google hacking pode ser usado para diversos fins e ataques específicos, por exemplo, procurar sites que exijam autenticação para testar ataques de SQL Injection.

Por isso, é muito importante seguir práticas seguras no desenvolvimento de uma aplicação web, implementar revisões de códigos e realizar a aplicação de configurações seguras nos servidores. Para o desenvolvimento de aplicações web, recomendamos uma consulta no projeto OWASP (Open Source Web Application Security Project), que possuí diversas dicas e práticas seguras de desenvolvimento.

FONTE: https://www.trustsign.com.br/portal/blog/entenda-o-google-hacking/

RESUMINDO:

• Google Hacking é a atividade de usar recursos de busca, visando atacar ou proteger melhor as informações de uma empresa.

• As informações disponíveis nos servidores web das empresas provavelmente estarão nas bases dedados do Google.

• Um servidor mal configurado pode expor diversas informações no Google. Não é difícil conseguir acesso a arquivos de base de dados de sites através do Google.

COMANDOS AVANÇADOS NO GOOGLE:

intitle, allintitle

Busca conteúdo no título (tag title) da página.

inurl, allinurl

Encontra texto em uma URL.

filetype

Busca por um arquivo de determinado tipo.

allintext

Localiza uma string dentro do texto de uma página.

site

Direciona a pesquisa para o conteúdo de um determinado site.

daterange

Busca por páginas publicadas dentro de um “range” de datas.

cache

Mostra a versão em cache de uma determinada página.

info

Mostra conteúdo existente no sumário de informações do Google.

related

Mostra sites relacionados.

Google Hacking Database

Há um banco de dados virtual, com tags de busca no Google previamente criadas para conseguir informações específicas.

Devemos manter em mente a possibilidade de adaptar tais tags de busca para nossas necessidades.

Um simples exemplo do que podemos encontrar no Google, e que pode voltar-se contra a pessoa que disponibilizou tais informações online, é o seguinte: digitar na caixa de busca currículo + cpf.

Exemplos de utilização, busca por arquivos de base de dados em sites do governo:

site:gov.br ext:sql

Busca por um servidor específico

inurl:"powered by" site:sistema.com.br

A pesquisa busca arquivos de e-mail em formato .mdb

inurl:e-mail filetype:mdb

Essa pesquisa busca telefones disponíveis em intranet encontradas pelo Google

inurl:intranet + intext:"telefone"

Realizando uma pesquisa dessa maneira é possível identificar muitos dos subdomínios da Oracle

site:oracle.com -site:www.oracle.com

Detectando sistemas que usando a porta 8080

inurl:8080 -intext:8080

Encontrando VNC

intitle:VNC inurl:5800 intitle:VNC

Encontrando VNC

intitle:"VNC Viewer for Java"

Encontrando Webcam ativa

"Active Webcam Page" inurl:8080

Encontrando Webcam da toshiba:

intitle:"toshiba network camera - User Login"

Encontrando Apache 1.3.20:

"Apache/1.3.20 server at" intitle:index.of

Asterisk VOIP Flash Interface

intitle:"Flash Operator Panel" -ext:php -wiki -cms -inurl:as

Dezenas de *dorks* são postadas semanalmente no http://exploit-db.com/google-hacking-database/ teste algumas como atividade prática.

Shodan

O Shodan é um motor de busca projetado por John Matherly, que embora seja classificado na mesma linha de soluções como Google e Bing indexa informações de maneira diferente dos líderes do mercado.

Motores de busca típicos procuram links associando-os às palavras, formando assim índices (indexação), o Shodan trabalha de maneira diferente, essa ferramenta “escaneia” portas e recolhe "*banner's*" de serviços que respondam através da internet ao invés de conteúdo web inserindo-os em seu índice.

O Shodan é projetado para ajudar usuários a encontrar nós específicos (desktops, roteadores, servidores, switches, câmeras) analisando informações retiradas do banner da aplicação.

Para utilizar o Shodan de maneira otimizada, alguns conhecimentos acerca do funcionamento desse buscador são necessários.

Inicialmente crie uma conta para utilizar o serviço, o login não é um requisito, entretanto opções de filtro só podem ser utilizados após o login.

OPERADORES BÁSICOS: FILTROS

country: filtra os resultados a partir do código de duas letras do seu país.

hostname: filtra os resultados especificando nomes de servidor ou domínio.

net: ordena por faixa de IP ou sub-rede.

os: busca por sistemas operacionais específicos.

port: busca por serviços específicos da porta informada.

A imagem mostra a busca de *webcams* no Brasil aplicando a *query* webcam country:BR

Você pode pesquisar por serviços vulneráveis ou antigos rodando em servidores ao redor do mundo, exemplo: apache 2.2.3

Pode também especificar domínios para a pesquisa, servidores Apache rodando em sites do governo: apache hostname:.gov.br ou iis-5.0 hostname:.gov.br

Os filtros Net / OS propiciam a busca por endereços IP e sistemas operacionais respectivamente, exemplo: country:BR OS:xp procura por máquinas XP no Brasil.

O filtro port como é de se imaginar filtra aplicações por porta podemos buscar serviços VNC no Brasil com a query: country:BR port:5900

Acesse o SHODAN clicando aqui: http://www.shodan.io e faça (se possível) consultas na sua empresa ou servidor próprio, lembre-se que acessar informações e equipamentos sem prévia autorização é considerado crime.

DEFCON 18: SHODAN for Penetration Testers 1/3: https://www.youtube.com/watch?v=EwDi2I3Q3yE