Capa

Slide 1 e 2 - Aviso
Todo conteúdo passado aqui é para fins educativos.
O uso para fins de causar dano, além de não ser o foco deste grupo, é crime.

Slide 3 - Google Hacking (ou Google Dorks)
É o método usado por 100% dos Script Kiddies e criadores de Botnet.
Com esta técnica você consegue scanear por possiveis sites vuneraveis, principalmente SQL Injection.
SQL Injection é uma tecnica em que o atacante literalmente injeta comandos SQL para conseguir acessar o Banco de Dados e, muitas vezes, ter acesso Administrador no Sistema.

Slide 4, 5, 6, 7 e 8 -
Ler slides

Slide 9 -
A grande sacada das Dorks é o uso combinado delas. Sabendo o que estamos procurando podemos direcionar nossa busca para isso.
Por exemplo: site:"sp.gov.br" inurl:".php?id=" irá procurar por possiveis vulnerabilidades de SQL Injection somente em sites do Governo de São Paulo, tanto Governo do Estado como Município.
Mudando o parametro "site:" para "eb.mil.br" retornará somente sites do Exército Brasileiro.
Tirando o 'eb' a busca fica mais generica, retornando sites não só do Exército como da Marinha e Aeronáutica.

Uma 'dork' que Eu acabei esquecendo de colocar nos slide é a 'intext:' que procura pelos parametros passados no corpo de texto dos sites. Por exemplo: intext:"a polícia apreendeu" retornará notícias sobre apreensões em geral.
Juntando tudo temos uma infinidade de possibilidades!

Visitando o Exploit DB, logo no Menu teremos o Google Hacking Database (https://www.exploit-db.com/google-hacking-database/) que é um Banco de Dados com um monte de 'dorks' conhecidas para vulnerabilidades em geral como SQLi, LFI/RFI, vulnerabilidades direcionadas a um Framework ou WebApp especifico bem como Devices de IoT como Cameras e HDs Externos com função 'Cloud'.

Um outro site que fiquei pensando se mostrava agora ou não, pois ele não é de 'Deus', é o Shodan (https://www.shodan.io/).
Nele você pode procurar por serviços e devices com alguns operadores avançados para filtrar por pais, porta, entre outros.
Procurando por MySQL/MariaDB? Use 'product:MySQL' que retornará banners capturados com esses Serviços.
Porta especifica? é pra já! port:502 (ModBUS)
Em algum pais especifico? country:BR

Um video do Dan Tentler, na Defcon 20, sobre o que ele já encontrou usando o Shodan - https://www.youtube.com/watch?v=5cWck_xcH64

Slide 10 - Whois
O whois é um serviço que pode retornar informações pessoais sobre donos de dominios, como CPF, telefone e email de contato.
Para sites no Brasil, podemos usar a ferramenta do Registro.br para tal: https://registro.br/2/whois
Digitando "bradesco.com.br" no campo de busca e dando enter, teremos algumas informações sobre os Contatos relacionados a esse Dominio, bem como os Servidores DNS que respondem por ele.
Aqui a brincadeira já fica interessante, pois podemos começar a mapear a Rede de nosso alvo.

Combinando com o que aprendemos de 'dorks' anteriormente nos possibilita sair um pouco do foco de vulnerabilidades em sites e passamos a pensar em

"vulnerabilidades em seres humanos". O que quero dizer com "vulnerabilidades em seres humanos" é a tática conhecida como 'phishing', principalmente na sua versão 'spear phishing'.
Phishing é o ato de enganar o usuário para clicar em um link malicioso ou enviar informações sensíveis. Você já deve ter visto aqueles emails de banco pedindo para você recasdatrar os códigos de segurança do seu cartão bancário. Isso é um Phishing. O Golpista envia a várias pessoas e, com alguma sorte, algumas delas enviam as informações.
Um "Spear Phishing" é um Phishing focado, direcionado a uma única pessoa, feito com base em informações coletadas sobre seus hábitos de consumo, por exemplo.
Pensando dessa forma, podemos forjar um email falso, com um link para uma página falsa, para enganar desde o Estagiário até o CEO de uma Empresa.
Como fazer isso? Escolhendo um alvo, uma empresa, por exemplo,
Combinando essas 'dorks' todas com uma pesquisa no Linkedin, Facebook, Twitter e Instagram.

Slide 11 - DNSRecon
É uma ferramenta para Enumeração de DNS que, dentre outras coisas, nos permite fazer:
- Checar todos os Registros NS de uma Zona de Transferência
- Enumerar os Registros Gerais de DNS de um domínio (MX, SOA, NS, A, AAAA, SPF e TXT)
- Checar por Resolução Coringas (Wildcard Resolution)
- Fazer procura por Registro PTR de uma faixa de IP ou CIDR
- Checar o cache de um Servidor DNS por registros A, AAAA e CNAME
- Enumerar registros mDNS Comum em uma Rede Local
- Enumerar Hosts e Subdomínios usando o Google

Video usado no slide: https://www.youtube.com/watch?v=YSkthF18Eo0
Página no Kali: http://tools.kali.org/information-gathering/dnsrecon