UFC

Universidade Federal do Ceará
Campus Quixadá
Segurança da Informação

Lab03

Docente:
Roberto Cabral Rabelo Filho

Discente:
Gregório Mariano de Azevedo Neto

Matricula:
402749

Maio
2021

Lab03

1 Módulo 1

1.1 Introdução

O método de invasão Pentest possibilita identificar pontos de falha dentro e fora das redes de uma empresa, com o objetivo de verificar as resistências das redes e se estão veneráveis a ataques.

2 Módulo 2

2.1 Google Hack

O Google Hacking é um método para encontrar falhas, arquivos e etc. Usa-se ele como uma espécie de scanner em cima do web crawler do Google, possibilitando buscas avançadas através de comandos.

- site: Este comando faz a busca em um site específico.
- allintitle: Faz a busca diretamente no título das páginas.
- allinurl: Busca conteúdos presentes na URL do site.

2.2 Script Pentest

Essa ferramenta ao ser inicializada. ela consegue copiar os comandos executado pelo terminal e mostrar todos comandos que foram executados quando é finalizada. Útil para gerar relatório.

2.3 TheHarvester

É uma ferramenta de coleta de informações, com ela é possível obter e-mails, subdomínios, hosts, nomes de funcionários, portas abertas, banners de diferentes fontes públicas, etc.

2.4 NetDiscover

O NetDiscover é uma ferramenta de varredura de rede para que serve para relacionar todos os hosts que estão ativos.

2.5 Whois e DNS

É um mecanismo que registra domínios, IPs e sistemas autônomos na Internet e que serve para identificar o proprietário de um site. Reúne todas as informações pertencentes a uma página.

2.5.1 DNSEnum

É uma ferramenta que possibilita obter informações de um determinado DNS.

2.6 Maltego

É uma ferramenta normalmente muito utilizada para buscar e relacionar informações que estão espalhadas pela internet. Detectando rastros deixados pelo atacante ou no caso do atacante encontrar vulnerabilidades ou informações sigilosas que não deveriam estar expostas.

3 Módulo 3

3.1 NMap

É uma ferramenta de segurança usada para detectar computadores e serviços numa rede, criando um "mapa" dessa mesma rede rede. Utiliza inúmeras técnicas de detecção, como:

- NMAP SO + TLL
- NMAP VARREDURA COMPLETA
- NMAP PORTAS
- NMAP SCRPIT

3.2 Exploit Database

É um site que lista e cria arquivos de todos os exploits encontrados e conhecidos em softwares comerciais.

4 Módulo 4

4.1 Nikto

É uma ferramenta desenvolvida para encontrar diversos tipos de arquivos, configurações e programas padrões ou inseguros, em servidores WEB. Onde tem como objetivo dar assessoria em servidores WEB, enquadrando-se na categoria de scanners de vulnerabilidades.

4.2 Nessus

É uma ferramenta de auditoria muito usada para detectar e corrigir vulnerabilidades em sistemas. Ele realiza uma varredura de portas, detectando servidores ativos e simulando invasões para detectar vulnerabilidades. Uma característica importante é que o Nessus procura por servidores ativos não apenas nas portas padrão, mas em todas as portas TCP.