LAB 03 - Pentest

Paulo Miranda e Silva Sousa[1] **- 400147**

[1]Universidade Federal do Ceará (UFC) – Campus Quixadá

paulomirandamss@alu.ufc.br

Pentest é método de invasão para encontrar vulnerabilidades em um sistema. Para isso, podemos usar várias ferramentas para auxiliar nessa tarefa.

1. Obtendo Informações

Para realizar um teste de penetração, primeiramente é necessário fazer um levantamento de informações. Para isso, podemos utilizar as seguintes ferramentas.

1.1. Script

Script é um programa que possibilita rastear todos os comandos e saídas executadas no terminal. É uma ferramenta muito útil para geração de relatório ao final do teste de penetração.

1.2. Google Hacking

O Google Hacking é uma técnica de busca usada para extrair informações da empresa que será testada.

1.2.1. site:

é um prefixo usado para buscar tudo sobre um determinado site. Ex: ”site: site:https://moodle2.quixada.ufc.br/”

1.2.2. allintitle:

é um prefixo usado para buscar palavras chaves no titulo de algum site. Ex: ”allintile: admin”

1.2.3. allinurl:

é um prefixo usado para buscar palavras chaves na url de algum site. Ex: ”allinurl: noticias.php?id=”

1.3. Theharvester

O Theharvester é uma ferramenta de busca para encontrar informações sobre um determinado domínio. Você pode especificar o domínio usando o -d, a quantidade de busca com -l e a fonte de busca com o -b. Ex: ”Theharvester -d google.com -l 200 -b bing”.

1.4. Netdiscover

O Netdiscover é uma ferramenta que possibilita fazer um levantamento dos dispositivos conectados na rede.

1.5. Whois e DNS

Com o comando whois é possível obter informações sobre o responsável por um determinado domínio.

Com o comando dnsenum é possível obter informações sobre um determinado DNS.

1.6. Maltego

O Maltego é uma ferramenta para organizar as informações que foram coletadas durantes as buscas.

2. Sondagem, Mapeamento e Identificação de Vulnerabilidades

Outra etapa importante do pentest é a sondagem, mapeamento e a identificação de vulnerabilidades. Para isso, podemos usar as ferramentas a seguir.

2.1. Nmap

O nmap possibilita fazer o levantamento dos hosts ativo na rede. Além dos hosts, ele mostrar os serviços e portas que estão disponíveis. Por fim, também é possível extrair informação sobre o sistema operacional.

2.2. Netcat

O comando nc é usado para descobrir as versões dos serviços em uma determinada porta.

2.3. Nikto

O Nikto é uma ferramenta usada para extrair informações sobre uma plataforma web.

2.4. Nessus

O Nessus é uma ferramenta paga utilizada para identificar falha e vulnerabilidade de sistemas.