
UNAERP
Universidade de Ribeirão Preto
Campus Ribeirão Preto · Campus Guarujá

Segurança da Informação

Tópicos Especiais em Engenharia

Ethical Hacking

Ferramentas para Varredura


PenTest
Teste de Intrusão / Penetração

Fases de um Pentest

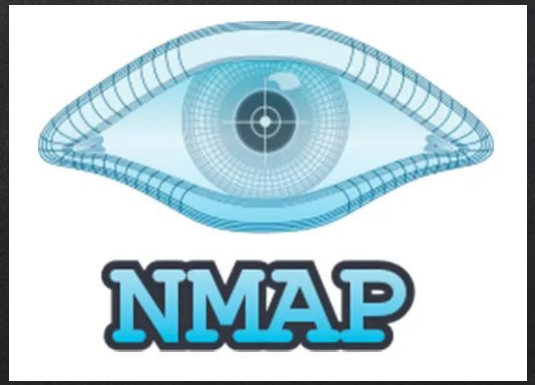
- ✘ Etapa 0 : Negociação
- ✘ Etapa 1 : Levantamento de dados (FootPrinting)
- ✘ Etapa 2 : Varredura
- ✘ Etapa 3 : Ganhando Acesso
- ✘ Etapa 4 : Mantendo Acesso
- ✘ Etapa 5 : Limpando Rastros
- ✘ Etapa 6 : Escrita de Relatórios

Etapa 1: Identificação ou Coleta de Dados

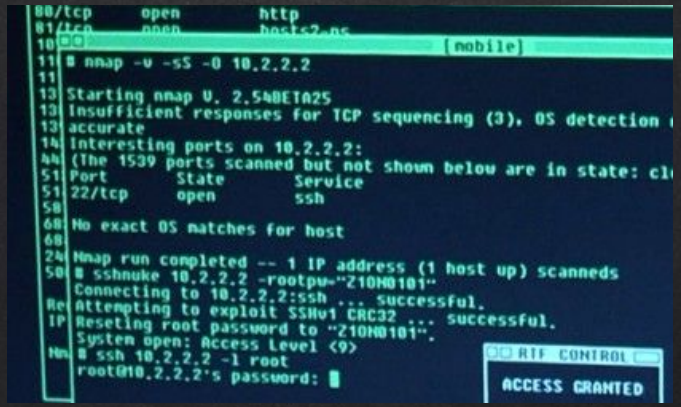
- Fontes que possam trazer informações sobre a empresa
  - softwares
  - sites
  - pessoas
  - livros
  - jornais
- Ferramentas
  - Maltego
  - AnyWho
  - Google Maps

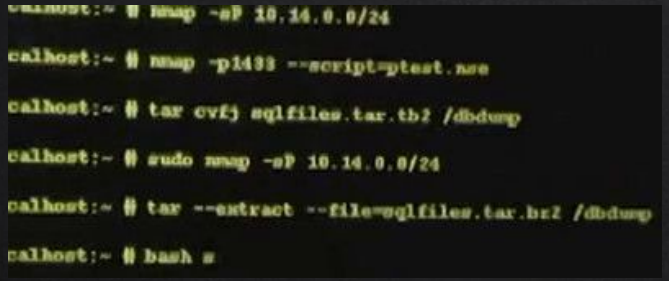
Etapa 2: Varredura

- Softwares/sites que fazem varreduras buscando por vulnerabilidades:
  - nmap
  - nslookup
  - Nessus
  - ping
  - nbtsat
  - macof
  - netdiscover
  - smbclient
  - SuperScan
  - Pstools
  - nikto
  - owasp-zap
  - Sqlmap
  - Google Hacking



- ✘ Network Mapper
- ✘ Desenvolvido por Gordon “Fyodor” Lyon (1997)
- ✘ Possui modo gráfico (Zenmap)
- ✘ Permite escanear portas de rede
  - avaliar segurança de um dispositivo na rede
  - descobrir serviços e portas abertas





https://nmap.org/movies/

NMAP - Comandos

- ✘ -sT : varredura completa de portas TCP
- ✘ -O : detecta SO
- ✘ -sU : varredura UDP
- ✘ -sO : varredura de IP
  - quais protocolos IP são suportados
- ✘ - sA: Varredura ACK: mapeia regras ativas no firewall

Nessus

- ✘ Cliente / Servidor
- ✘ Verificação de falhas e vulnerabilidades
- ✘ https://temp-mail.org/
- ✘ Relatórios

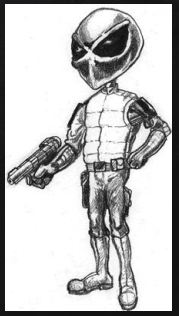
Owasp Zap

- ✘ OWASP (Open Web Application Security Project)
- ✘ ZAP (Zed Attack Proxy)
- ✘ Automatizar testes
  - https://pypi.org/project/python-owasp-zap-v2.4/
- ✘ Ataque Spider
  - https://www.zaproxy.org/docs/desktop/start/features/spider/
- ✘ Active Scan
  - requests e respostas resultantes de varredura ativa de um site

DirBuster

- ✘ Também desenvolvida pela OWASP
- ✘ Dicionários
  - Dicionários pré-existentes
  - /opt/DirBuster/ ou /usr/share/dirbuster/wordlists
- ✘ Brute-force puro
  - Conjunto de caracteres deseja que sejam utilizados
  - Quantidade mínima e máxima de caracteres por tentativa.

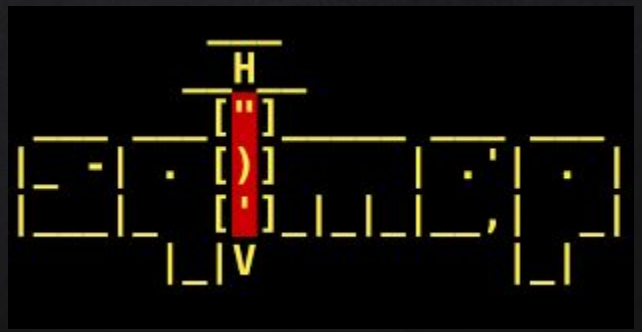
Nikto



- ✘ Escrito em PERL
- ✘ Análise de vulnerabilidades comuns em servidores Web
- ✘ nikto –h http://testphp.vulnweb.com
- ✘ nikto –h http://testphp.vulnweb.com –evasion 1,2,3 –o relatorio.html

SQLMAP

- ✘ Open-source
- ✘ Python
- ✘ SQL Injection
- ✘ Procurar parâmetros via GET



SQL MAP - Comandos

- ✘ sqlmap -u URL --dbs
- ✘ sqlmap -u URL -D NOME_BASE --tables
- ✘ sqlmap -u URL -D NOME_BASE -T NOME_TABELA --dump

Atividade

- ✘ Utilizar uma das ferramentas apresentadas
  - se possível, via Kali Linux em VMWARE
    - https://www.kali.org/downloads/
    - Kali Linux 64-bit VMware
- ✘ Pesquisar vulnerabilidades no site http://testphp.vulnweb.com
  - ou em um dos sites do http://www.vulnweb.com/
- ✘ Escrever um breve relatório sobre uma vulnerabilidade encontrada
  - impactos
  - possíveis formas de correção
- ✘ 1 página

DÚVIDAS?

- ✘ Não esqueça de enviar sua maior dúvida pelo link que está no ClassRoom.
- ✘ Críticas/Sugestões: ezarpelao@unaerp.br

Credits

Special thanks to all the people who made and released these awesome resources for free:

- ✘ Presentation template by SlidesCarnival
- ✘ Photographs by Unsplash