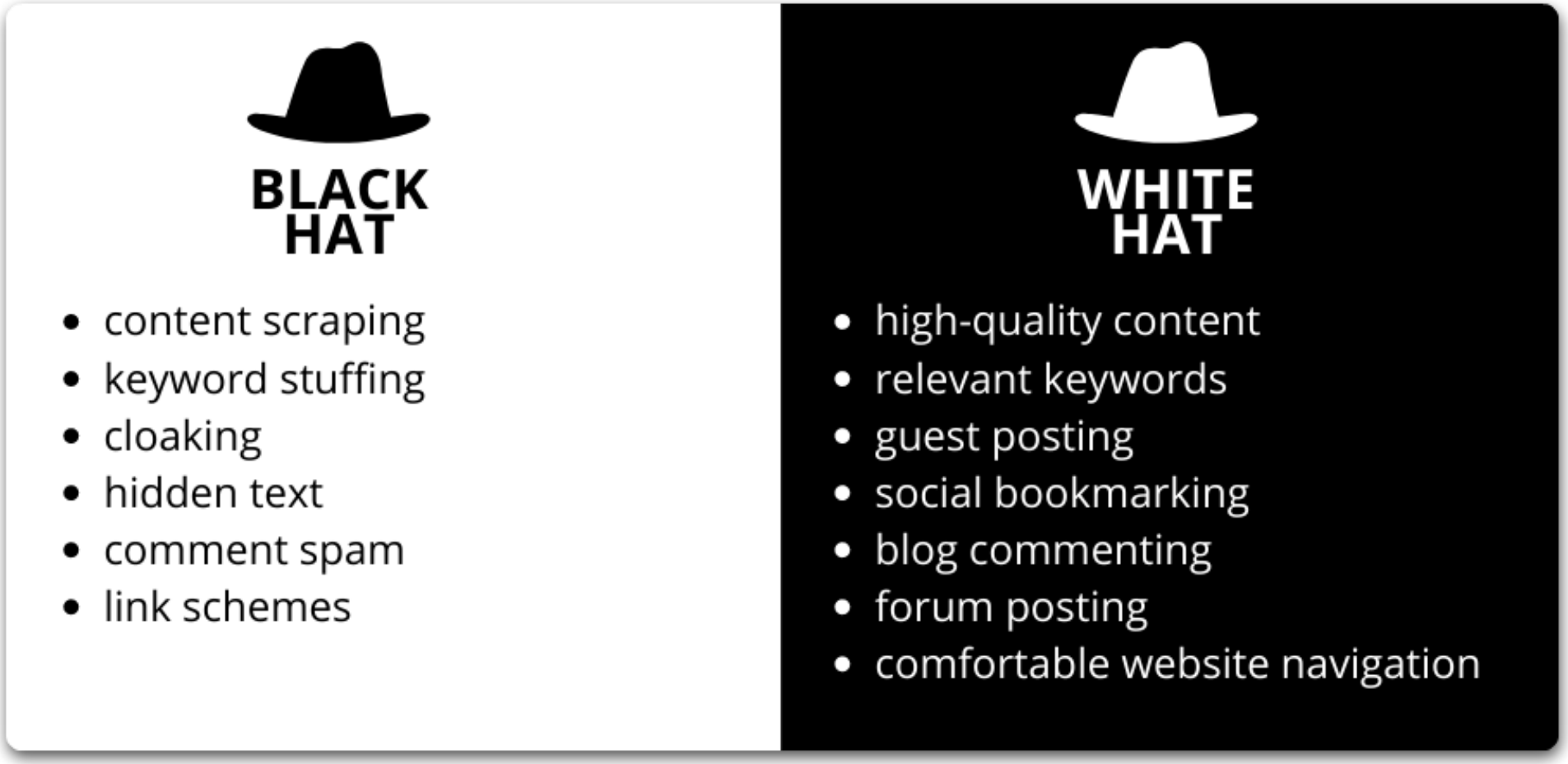
EMENTA

- Introdução ao Hacking Pentest
- Instalação do Kali Linux
- Footprinting
- Nmap
- Port Scanner
- Reconhecimento web e vulnerabilidades
- SQL Injection
- Bypass CloudFlare
- Shell Upload
- Reverse Shell
- Post Exploitation e Hashs
- Criptografia
- Privilege Escalation
- Pivoting de redes corporativas

PENTEST?


BLACK HAT
content scraping
keyword stuffing
cloaking
hidden text
comment spam
link schemes
WHITE HAT
high-quality content
relevant keywords
guest posting
social bookmarking
blog commenting
forum posting
comfortable website navigation

AS FASES DO PENTEST

- Definição do escopo e coleta de informações
- Análise de vulnerabilidade
- Exploração
- Pós exploração
- Relatório

MERCADO DE TRABALHO (1/2)

- Profissões
  - Pentest
  - Analista de segurança / redes
  - Perito forense computacional
  - Pesquisador de vulnerabilidades
  - Consultor em segurança
  - Chefe/Diretor de segurança (CSO)
  - Desenvolvedor
  - Espionagem / Contra-espionagem

MERCADO DE TRABALHO (2/2)

- Certificações
  - ISSO 27000 / ISSO 27002
  - CompTIA – Security+
  - Cisco Systems – CCNA / CCNA Security / CCSP / CCIE Security
  - EC-Council – CEH / CHFI / ECSA / ENSA / LPT
  - ISACA – CISA / CISM
  - $(ISC)^2$ - CAP / CISSP / CSSLP / ISSAP / ISSEP / ISSMP / SSCP
  - ISECOM – OPSA / OPST
  - Offensive Security – OSCP / OSCE

QUALIDADES E HABILIDADES

- Ética e transparência
- Inglês
- Curiosidade
- Gostar de desafios
- Persistência
- Resolver problemas
- Disciplina e estudos